NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE MILLENNIAL GENERATION AS AN INSIDER THREAT: HIGH RISK OR OVERHYPED?

by

David J. Fisher

September 2015

Thesis Co-Advisors: Carolyn Halladay
Fathali Moghaddam

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2015	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE THE MILLENNIAL GENERATION AS AN INSIDER THREAT: HIGH RISK OR OVERHYPED?			**5. FUNDING NUMBERS**
6. AUTHOR(S) Fisher, David J.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Cyber security experts agree that insider threats are and will continue to be a threat to every organization. These threats come from trusted co-workers who, for one reason or another, betray their organizations and steal data, disrupt information systems, or corrupt the data. Millennials are commonly thought of as entitled, high maintenance, and less trustworthy than the older generations; in other words, they have personality traits associated with insider threats, making the insider threat and the Millennial a dangerous combination. But are the Millennials truly any more likely to become insider threats than members Generation X (GenX) or Baby Boomers?

This study shows that, contrary to conventional wisdom and societal belief, Millennials are no more likely to become insider threats than other generations; in fact, data shows they are less likely to do so than members of GenX.

14. SUBJECT TERMS insider threat, cyber security, millennial, baby boomer, Gen X, Generation X			**15. NUMBER OF PAGES** 109
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01-280-5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE MILLENNIAL GENERATION AS AN INSIDER THREAT: HIGH RISK OR OVERHYPED?

David J. Fisher
Program Manager, Department of Homeland Security
B.S., California State University of Pennsylvania, 1989

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2015**

Approved by: Carolyn Halladay, Ph.D.
Thesis Co-Advisor

Fathali Moghaddam, Ph.D.
Thesis Co-Advisor

Mohammed M. Hafez, Ph.D.
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Cyber security experts agree that insider threats are and will continue to be a threat to every organization. These threats come from trusted co-workers who, for one reason or another, betray their organizations and steal data, disrupt information systems, or corrupt the data. Millennials are commonly thought of as entitled, high maintenance, and less trustworthy than the older generations; in other words, they have personality traits associated with insider threats, making the insider threat and the Millennial a dangerous combination. But are the Millennials truly any more likely to become insider threats than members Generation X (GenX) or Baby Boomers?

This study shows that, contrary to conventional wisdom and societal belief, Millennials are no more likely to become insider threats than other generations; in fact, data shows they are less likely to do so than members of GenX.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
A. BACKGROUND 3
B. PROBLEM STATEMENT 4
C. RESEARCH QUESTION 9
D. LITERATURE REVIEW 10
1. Who Is an "Insider" and What Is the Threat? 10
2. Generations: What's in a Name? 12
E. METHODOLOGY 16
F. CHAPTER OVERVIEW 19

II. THE INSIDER THREAT 21
A. DEFINITIONS 21
B. MOTIVATION 22
C. US-CERT RISK FACTORS 25
D. CHARACTERISTIC ANALYSIS 26
E. CONCLUSION 36

III. ANALYSIS 39
A. DATA ANALYSIS METHODS 39
B. ESTABLISHING THREAT HIERARCHY 39

IV. INSIDER THREAT STATISTICS 61

V. CONCLUSION 69
A. CRITICAL ASSESSMENT 71
B. CONCLUSION 73

BIBLIOGRAPHY 75

INITIAL DISTRIBUTION LIST 87

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Types of Crime Committed by Insiders 62
Figure 2. Industries Attacked by Insiders 63
Figure 3. Generational Insider Threat Percentages 64
Figure 4. Generational Workforce Percentages 65
Figure 5. Millennial Breakdown 66
Figure 6. BabyBoomer Breakdown 66
Figure 7. Traditionals Breakdown 67
Figure 8. GenX Breakdown 67

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Greed/Financial Need Applicability 40
Table 2. Compulsive and Destructive Behavior Applicability 42
Table 3. Introversion Applicability 43
Table 4. Rebellious, Passive Aggressive Applicability 45
Table 5. Ethical “Flexibility” Applicability 46
Table 6. Reduced Loyalty Applicability 48
Table 7. Entitlement/Narcissism (Ego/Self-image) Applicability 49
Table 8. Minimizing Their Mistakes or Faults Applicability 50
Table 9. Inability to Assume Responsibility for Their Actions Applicability 51
Table 10. Intolerance of Criticism Applicability 52
Table 11. Self-perceived Value Exceeds Performance Applicability 53
Table 12. Empathy Applicability 54
Table 13. Predisposition toward Law enforcement (Authority) Applicability 55
Table 14. Raw Tabulation 56
Table 15. Weighted Tabulation 57
Table 16. Percentage of Compromises Compared to Workforce Population 70

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CERT	Carnegie Mellon's Computer Emergency Response Team
DHS	Department of Homeland Security
DOD	Department of Defense
EEOC	Equal Employment Opportunity Commission
ERC	Ethics Resource Center
FBI	Federal Bureau of Investigation
GCHQ	Government Communication Headquarters
GenX	Generation X
IT	Information Technology
NCCIC	National Cybersecurity and Communications Integration Center
NITTFMFS	National Insider Threat Task Force Mission Fact Sheet
NSA	National Security Agency
ODNI	Office of the Director of Intelligence
PERSEREC	DOD Personnel and Security Research Center
US-CERT	United States Computer Emergency Readiness Team

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

This thesis asks if a specific generation, Millennials, is collectively more likely to possess the characteristics and traits of an insider threat than the Baby Boomers or Generation X (Gen X) generations. For the purposes of this study, insider threat it is defined as "people who maliciously and deliberately used their access to cause harm."[1] The study's relevance lies in the fact that these three generations comprise 95 percent of today's workforce, with the Millennials steadily becoming the largest part.[2]

This analysis is accomplished by comparing the generations against known insider threat risk factors. These risk factors, as defined by the United States Computer Emergency Readiness Team (US-CERT), are:

- greed/financial need
- entitlement—narcissism (ego/self-image)
- ethical "flexibility"
- vulnerability to blackmail
- reduced loyalty
- rebelliousness, passive aggressiveness
- compulsiveness and destructive behavior
- introversion
- lack of empathy
- predisposition toward law enforcement (authority)
- minimization of their mistakes or faults

[1] Eric Cole, *Insider Threats in Law Enforcement* (Bethesda, MD: SANS Institute 2014), http://www.sans.org/reading-room/whitepapers/analyst/insider-threats-law-enforcement-35402.

[2] The traditional generation, born before 1945, represents 5 percent of the US workforce as of 2012. That percentage continues to shrink as those workers exit the workforce. See "Generations" Demographic Trends in Population and Workforce," Knowledge Center, March 5, 2013, http://www.catalyst.org/knowledge/generations-workplace-united-states-canada.

- intolerance of criticism
- inability to assume responsibility for their actions
- self-perceived value exceeding their performance[3]

Each of these factors is analyzed to identify which generation possesses which factors, creating the generation's insider threat probability. Then each generation is ranked to develop the generation threat hierarchy—that is, the order in which the generations rank relative to their possession of insider threat risk factors. The threat hierarchy then provides the theoretical answer to the research question.

The data sources utilized for this study stem from a variety of functional areas, disciplines, and organizations. The insider motivations are gathered through various behavioral analysis studies from US-CERT, the Federal Bureau of Investigation (FBI), Department of Defense's Personnel and Security Research Center (PERSEREC) and published, first-hand accounts and descriptions of known insiders and those who encourage them.[4] The data used for enumerating successful insider threat compromises was provided by Carnegie Mellon's Computer Emergency Response Team (CERT).[5] This data has been collected and tabulated since 1996 to capture a variety of data points about successful insider threat attacks. It validates the theoretical answer based on a comparison of actual data sets.

[3] National Cybersecurity and Communications Integration Center, Combating the Insider Threat (Washington, DC: U.S. Department of Homeland Security, 2014), https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat.pdf.

[4] The United States Computer Emergency Readiness Team (US-CERT) is an organization within the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD). It is accepted among cyber security practitioners as an authoritative agency relative to all elements of cyber security and defenses.

[5] Not to be confused with US-CERT, which is part of the federal structure, CERT is a "national asset in the field of cybersecurity that is recognized as a trusted, authoritative organization dedicated to improving the security and resilience of computer systems and networks." See "About Us," Software Engineering Institute, accessed August 23, 2015, https://www.cert.org/about/.

This study shows three results. First, despite the stereotypes, Millennials are no more likely to be insider threats than any other generational cohort. Second, based simply on the projected representation in the workforce, Millennials may still become the primary perpetrators of insider threat attacks in the workforce. Lastly, as their numbers in the workforce continue to grow, Millennials will likely be the majority of the perpetrators in the years to come; statistically, however, there is no reason to believe that the percentage of attacks from Millennials will increase any more than what is currently experienced.

During the course of researching, analyzing, and writing on this topic, it became apparent that there are several shortcomings that, while certainly affecting the outcome to a minor extent, are not believed to cast any significant doubt on the findings: the weight assigned to the risk factors that led to the calculations, the data used in the analysis, and the analysis' limited scope. Weight was assigned to factors based on input from available literature, which included both academic publications and online material. As sparse as the available information was, the category weights represent the best estimates.

The second shortfall is regarding the data used in the analysis. The data provided by CERT has merit, however CERT possesses no authority to require any organization, private of public, to report any breaches related to cyber security, let alone specifics regarding compromises that can be traced directly to an insider threat. The data reaches back to 1997 and consists of 655 reported cases of insiders stealing data from within an organization's information systems. While a larger dataset would strengthen the analysis' validation, this study could only use what was made available by CERT.

Lastly, the scope of this analysis is limited to the generational cohorts. Furthering this study by breaking the cohorts into more specific demographics such as age, race, gender, and level of education, while not providing significant validation to the findings, might lend further insight into the Millennial cohort itself to specifically determine which combination of demographics warrants further research. This thesis shows that Millennials are statistically less likely to become

insider threats; deeper examination into the generation's demographics is the next logical step.

This thesis asked the question: Do Millennials pose a higher risk of becoming insider threats? Based on available evidence, the answer appeared to be that they are, in fact, more likely. The actual data, however, did not support the evidentiary conclusion. To the cyber security community, this finding means that, while Millennials have committed insider threat crimes below their representative workforce percentage, they will soon outnumber other generations; their lower-than-proportionate level of compromises will outnumber other cohorts simply by their sheer numbers. Thus, a successful mitigation strategy should be developed, keeping this finding at the forefront of the strategy— not because Millennials are more likely to compromise, but because they are simply more numerous.

ACKNOWLEDGMENTS

First and foremost, I want to thank God for providing me the strength and ability to complete this journey. With His strength, I can accomplish anything.

Next, thanks to my wife, Samantha, and my children, DJ, Mick, Josh, and Brianna. You are what drives me. You suffered through countless evenings and weekends of “I need to work on school stuff” keeping me from participating in fun activities with you (especially a vacation to the most magical place on earth), causing me to miss sporting events and generally taking time away from all of you.

Next, I would like to express my gratitude to my thesis committee, Dr. Carolyn Halliday and Dr. Fathali Moghaddam, who guided me down the road to thesis completion, providing me guidance when needed, yet allowing me the freedom to try, and occasionally fail, on my own.

Lastly, I wish to express my gratitude to my friends, colleagues, and chain of command. This group of people believed in me, backed my desire to take this journey, provided me the ability to complete the coursework, endured my frustration and stress, and provided support through this long process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> The young people of today think of nothing but themselves. They have no reverence for parents or old age. They are impatient of all restraint. They talk as if they alone knew everything and what passes for wisdom with us is foolishness with them. As for the girls, they are forward, immodest and unladylike in speech, behavior and dress.
>
> —Aristotle, circa 320 BC

In 2013, in Room 1014 of the Kowloon Mira hotel—a modern structure in the heart of Hong Kong's tourist district—sat a wiry, bespectacled National Security Agency (NSA) computer security contractor. He was joined by two staff members of the UK's *Guardian* newspaper—Ewen MacAskill and Glenn Greenwald. Greenwald believed the thin NSA man was too young to be the contact he expected to meet with; perhaps he was the source's son, or maybe his assistant.

The young man, however, Edward Snowden, was the source. And the information that he divulged to his hand-picked audience marked an unprecedented security leak. He had access to thousands of documents taken from the NSA and the UK's Government Communication Headquarters (GCHQ).[6] Most were classified top secret or higher. They told the story of NSA intercepting fiber optic cable communications that ringed the world, being able to bug anyone, collecting metadata on millions of Americans' phone records, email headers, and subject lines. More shocking, he spun a tale of a complicit Silicon Valley—with Google, Microsoft, Facebook, and even Apple, offering direct access into the technology behemoth's servers. It had "even put secret back doors into online

[6] "GCHQ is a security and intelligence organization tasked by government to protect the nation from threats." See "Who We Are," GCHQ, accessed August 25, 2015, http://www.gchq.gov.uk/who_we_are/Pages/index.aspx.

encryption software used to make secure bank payments, [effectively] weakening the system for everybody."[7]

Publication of these sensitive details has left the U.S. intelligence community reeling, and continues to color the national security discourse in the United States and among America's allies today. Many homeland security experts, however, consider Snowden to be reckless, naive, and dangerous—a man with the skills and the clearances that gave him access to some of the nation's most sensitive secrets, giving him the capability to put the lives of U.S. troops and intelligence operators at risk.[8]

At the time of Snowden's action, the public's trust in government hovered near an all-time low; in a Pew Research Center poll, 20 percent or respondents indicated they trust the government, while 79 percent said they distrust it.[9] For his part, Snowden believes he is a patriot and hero and he is widely and diversely celebrated among "hacktivists," conspiracy theorists, civil-libertarian absolutists, whistle-blowers, and skeptics of the post-9/11 "national security state." Snowden felt the programs he was exposing were illegal and posed a threat to the individual liberties on which this country was founded. He "reported these clearly problematic programs to more than ten distinct officials, none of

[7] Luke Harding, "How Edward Snowden Went from Loyal NSA Contractor to Whistleblower," *Guardian*, February 1, 2014, http://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract.

[8] Jeffry Toobin, "Edward Snowden Is No Hero," *New Yorker*, June 10, 2013, http://www.newyorker.com/news/daily-comment/edward-snowden-is-no-hero' James Gordon Meek, Luis Martinez, and Alexander Mallin, "Intel Heads: Edward Snowden Did 'Profound Damage' to U.S. Security," ABC News, January 29, 2014, http://abcnews.go.com/Blotter/intel-heads-edward-snowden-profound-damage-us-security/story?id=22285388; Erin McClam, "'Naive and Gravely Mistaken': Analysts Rebut Snowden Claims," NBC News, May 28, 2014, http://www.nbcnews.com/feature/edward-snowden-interview/naive-gravely-mistaken-analysts-rebut-snowden-claims-n117101.

[9] Michael Dimock et al., *Beyond Red vs. Blue: The Political Typology* (Washington, DC: Pew Research Center, 2014), http://www.people-press.org/files/2014/06/6-26-14-Political-Typology-release1.pdf.

whom took any action to address them."[10] After the attempts to have his concerns heard through official channels failed, he took it upon himself to make these programs public.

A. BACKGROUND

Snowden speaks to—and to some extent for—the generation known as Millennials, born from the early 1980s through the early 2000s. More than any other budding generation in recent decades, Millennials are uniquely distinctive: they are more numerous, affluent, and educated.[11] They embrace diversity far more than any other generation. They exhibit positive social habits that older Americans do not associate with youth. They are far more generous with their time and money, according to a Walden university study.[12] According to authors William Strauss, a historian, and Neil Howe, a historian and demographer, "Over the next decade, the Millennial generation will entirely recast the image of youth from downbeat and alienated to upbeat and engaged—with potentially seismic consequences for America."[13] They are also reputed to be "high-maintenance," to want to achieve high rank or status without paying their dues at the entry level first, and, as the Snowden case makes clear, to have an aversion to secrets and secret-keeping.[14]

---

[10] "Snowden: I Raised NSA Concerns Internally over 10 Times before Going Rogue," *Washington Post*," March 7, 2014, http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/07/snowden-i-raised-nsa-concerns-internally-over-10-times-before-going-rogue/?Post+generic=%3Ftid%3Dsm_twitter_washingtonpost.

[11] "5 Workplace Stereotypes about Millennials That Aren't True," U.S. News, March 16, 2015, http://money.usnews.com/money/blogs/outside-voices-careers/2015/03/16/5-workplace-stereotypes-about-Millennials-that-arent-true.;"What You Think about Millennials Is Wrong - The Washington Post," accessed July 7, 2015, http://www.washingtonpost.com/blogs/on-leadership/wp/2015/02/23/what-you-think-about-Millennials-is-wrong/.

[12] "Social Change impact Report," Walden University, 2011, http://www.waldenu.edu/~/media/Files/WAL/about/walden-university-social-change-impact-report-summary-report.pdf.

[13] William Strauss and Neil Howe*, Millennials Rising: The Next Great Generation* (New York: Random House, 2009).

[14] "Millennials Rising: Coming of Age in the Wake of the Great Recession." New America, June 16, 2015, 2014. http://www.newamerica.org/downloads/Millennials_Rising_Coming_of_Age_in_the_Wake_of_the_Great_Recession.pdf.

As technology continues to advance and improve, its convenience is interwoven inextricably into everyday life, continually transforming the world in which we live. Technology is an economic driver as well as a multiplier, providing organizations with convenient, reliable, and affordable ways to communicate, collaborate, and deliver a variety of goods and services. The Millennials are, as a group, very much at home with advanced and advancing technology.

With this progress, the increased and proportionate dependence on cyberspace relative to the homeland security mission underscores the dangers of malicious insiders disrupting agencies' abilities to perform homeland security tasks to accomplish their mission. While malicious actors routinely try to disrupt the government's day-to-day activities, cyber security experts are fighting to defend cyberspace and to ensure the nation's security is not affected by such attacks.

B. PROBLEM STATEMENT

This section discusses the four broad archetypes of the insider threat, providing some well-known and relevant examples of each.

The first archetype is the workplace (or school) massacrist who, as the tragic-cynical turn of popular phrase has it, "goes postal."[15] For example, on September 16, 2013, Aaron Alexis entered Building 197 in the U.S. Navy Yard in Washington, DC and began shooting. One hour later, after murdering 12 of his co-workers, Alexis was killed by responding officers in a firefight. Alexis fits the

[15] The term "going postal" dates at least to the early 1990s—see, for example, Karl Vick, "Violence at work tied to loss of esteem," *St. Petersburg Times*, December 17, 1993. The phrase entered the American vocabulary after a series of workplace-rage incidents involving postal workers or post offices in the 1980s. So prevalent was the idea that post offices were cauldrons of pent-up frustration that the U.S. Postal Service in 2000 commissioned a study on workplace safety—The National Center on Addiction and Substance Abuse at Columbia University, On the one hand, the study concluded: "Postal workers are no more likely to physically assault, sexually harass, or verbally abuse their coworkers than employees in the national workforce [and p]ostal employees are only a third as likely as those in the national workforce to be victims of homicide at work" (1). On the other hand, the same report found "Postal employees are six times likelier to believe they are at greater risk than the average worker to be a victim of workplace violence from co-workers (17 versus 3 percent), despite similar rates of violence by coworkers" (3-4). Either way, the figure of the disgruntled and homicidal coworker has become something of a stock character in American popular culture. http://permanent.access.gpo.gov/lps12068/33994.pdf.

description of a classic insider threat—a disgruntled worker who brings physical violence to his place of employment. The 34-year-old worked as a contractor with Hewlett-Packard Enterprise Services, which provided support to the U.S. Navy and Marines.[16] He passed a background investigation, and he was subsequently awarded a secret security clearance, which he maintained from March 2008 until the shooting.[17] This clearance made it easy for him to access the Navy Yard.

Alexis' case echoed the killing spree of Major Nidal Hassan, the Fort Hood shooter.[18] While their attacks' motivations differed, they both were trusted by their employers and co-workers and, in an instant, they betrayed this trust in rage-filled incidents of workplace violence resulting in numerous fatalities.

The second insider threat archetype is the classic spy, lurking in the shadows, who steals some type of data, be it financial or intelligence-related. In 1984, while working in the Naval Intelligence Support Center in Suitland, Maryland, Samuel Morison approached a co-worker's vacated desk and, seeing photographs of a Soviet nuclear aircraft, seized the opportunity and stole them. Morison trimmed the photos to remove the security classifications, and then sent it to *Jane's Defense Weekly*,[19] where it was ultimately published as the cover photograph for the August 1984 edition. For his deeds, Morison was later

[16] "Washington Navy Yard Gunman Aaron Alexis Was Hewlett-Packard Subcontractor," *Guardian*," accessed February 8, 2015, http://www.theguardian.com/world/2013/sep/16/aaron-alexis-washington-navy-yard-shooting.

[17] Kathleen Miller and Gopal Ratnam, "Shooter with Clearance Post-Arrest Exposes Vetting Gaps," Bloomberg Business, September 18, 2013, http://www.bloomberg.com/news/articles/2013-09-18/shooter-with-clearance-post-arrest-exposes-vetting-gaps.

[18] "Army: Fort Hood Gunman in Custody after 12 Killed, 31 Injured in Rampage," Fox News, November 6, 2009, http://www.foxnews.com/story/2009/11/06/army-fort-hood-gunman-in-custody-after-12-killed-31-injured-in-rampage.html; http://www.nytimes.com/2013/08/29/us/jury-weighs-sentence-for-fort-hood-shooting.html?_r=1&. Nidal Hassan is a U.S. Army Major and physiatrist who, fearing an impending war deployment, opened fire on soldiers in a pre-deployment center on November 5th, 2009 leaving 12 dead and wounding 32. On August 23, 2013 Hassan was convicted of 12 counts of premeditated murder and 32 counts of attempted murder in a military court martial. He was sentenced to death by lethal injection on August 28th, 2013

[19] Jane's Defense Weekly is a guide to international weapons technology and military defense news.

convicted of espionage and theft and was sent to prison.[20] The government, however, did not claim that any particular damage resulted from Morison's disclosure. Rather, the government maintained that future similar disclosures could provide the Soviets with data that would allow them to increase their knowledge of the American satellite surveillance system.[21]

Other well-known cases of insider spying include Robert Hanssen[22] and Aldrich Ames,[23] selling secrets to foreign powers more for their own gain in status and prestige than for any particular ideological affinities.

With the information age's various advances, opportunities, and challenges, new insider threats have emerged as well. The third archetype, the unintentional insider threat, is a regular computer user who, despite training and warnings and with no malicious intent, does something or fails to do something that causes harm to an organization's information systems—and to the data on which it relies. Typically, this is damage done through such social engineering attacks as phishing or web redirection. In December 2013, for example, up to 40 million Target customers who "made purchases by swiping their cards at terminals in its U.S. stores" may have had their data compromised.[24] Investigations discovered over 110 million customer accounts were compromised

[20] He served almost eight months of a two-year sentence before he was paroled.

[21] Robert F Ladenson., "Scientific and Technical Information, National Security, and the First Amendment: A Jurisprudential Inquiry," *Public Affairs Quarterly* 1, no. 2 (April 1987): 1–20. http://www.jstor.org/stable/40435639.

[22] "Robert Hanssen is a former US Federal Bureau of Investigation (FBI) agent who spied for Soviet and Russian intelligence services against the United States for 22 years from 1979 to 2001. He is serving a life sentence." "Robert Philip Hanssen Espionage Case," FBI, February 20, 2001, http://www.fbi.gov/about-us/history/famous-cases/robert-hanssen.

[23] Aldrich Ames is a former employee of the Central Intelligence Agency convicted, along with his wife, on charges of conspiracy to commit espionage on behalf of the former Soviet Union. "An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence," Senate Select Committee on Intelligence, November 1, 1994, Part One, http://www.fas.org/irp/congress/1994_rpt/ssci_ames.htm.

[24] "Target Says 40 Million Credit, Debit Card Accounts May Be Affected by Data Breach," Fox News, December 19, 2013, http://www.foxnews.com/us/2013/12/19/target-says-40m-accounts-may-be-affected-by-data-breach/.

in the attack.[25] Investigators found that this breach was caused by a heating, ventilation, and air-conditioning (HVAC) subcontractor who could connect to Target's network falling victim to a phishing email scam, which initiated the breach. While Target has never release the financial damage caused by the breach, the cost to replace the cards alone was in excess of $200 million.[26]

Similarly data-oriented, the last archetype is the malicious insider. This person, usually with elevated rights and privileges to a system, willfully and intentionally performs specific actions aimed at the organization's information systems to impact its confidentiality, integrity, availability, or any combination.[27] Private Bradley (now Chelsea) Manning was an intelligence analyst in the U.S. Army who, in July 2013, was convicted by a military court of violating the Espionage Act, among other offenses.

Manning stole and ultimately released the largest amount of military data to date—and in one of the most public demonstrations of the new kind of insider threat.[28] In January 2010, Manning downloaded more than 400,000 documents, known as the "Iraq War Logs."[29] Several days later, Manning downloaded another 91,000 documents, known as the "Afghan War Logs."[30] These logs "detail how soldiers, civilians, insurgents, foreign aid workers, private contractors, old men and young girls, Americans, Britons, foreign Arabs and above all, the Iraqi people themselves, fell victim to a new dynamic of 'asymmetric warfare,' in which guerrillas armed mainly with improvised landmines competed with the

[25] Dan Goodin, "Epic Target Hack Reportedly Began with Malware-Based Phishing E-Mail," Ars Technicm, February 12, 2013, http://arstechnica.com/security/2014/02/epic-target-hack-reportedly-began-with-malware-based-phishing-e-mail/.

[26] "Target Hack Cost Banks over $200M," TheHill, accessed January 5, 2015, http://thehill.com/policy/technology/198634-target-hack-cost-banks-over-200m.

[27] Michelle Keeney et al, *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors* (United States Secret Service and Carnegie Mellon University, May 2005), , http://www.secretservice.gov/ntac/its_report_050516.pdf.

[28] Kevin Poulsen and Kim Zet, "WikiLeaks' 400,000 Iraq War Documents Reveal Torture, Civilian Deaths," Wired, October 10, 2010, http://www.wired.com/2010/10/wikileaks-press/.

[29] Ibid.

[30] David Leigh, "Iraq War Logs: An Introduction, World News," *Guardian*, October 22, 2010, http://www.theguardian.com/world/2010/oct/22/iraq-war-logs-introduction.

awesome weaponry of hi-tech U.S. air power."[31] Manning saved this material on CDs, then copied it onto a personal laptop, and ultimately released those logs to WikiLeaks.[32] Manning, like Snowden, claims to have acted in the interests of peace and order in the world—essentially betraying the nation to save the nation.[33] Manning was only 25 years old.

This thesis focuses on the malicious insider threat, not least because the incidence of them is rising, along with the proportion of Millennials in the workforce.[34] Current projections regarding the percentage of Millennials in the work force vary; some estimate Millennials will comprise the majority of the workforce as soon as 2015; others, such as *Forbes*, posit that some 46 percent of the workforce will be Millennials by 2020, and 75 percent by 2015.[35] All observers agree that, as the years progress, the percentage of Millennials in the workforce will increase, and become the majority.

Couple this demographic shift with government and industry's increasing reliance on data, and information systems' growing vulnerabilities to insiders who know their way around the computer systems, and the treat becomes even plainer. If, as the malevolent insiders believe, data is money and/or power, the

---

[31] Ibid.

[32] Mark Clayton, "Bradley Manning Case Signals US Vulnerability to 'Insider' Cyberattack," The Christian Science Monitor, December 22, 2011, http://www.csmonitor.com/USA/2011/1222/Bradley-Manning-case-signals-US-vulnerability-to-insider-cyberattack.

[33] Chase Madar, "WikiLeaks, Manning and the Pentagon: Blood on Whose Hands?," *Al Jazeera*, June 20, 2014, http://www.aljazeera.com/indepth/opinion/2012/01/2012121123135872284.html.

[34] Andrew Horbury, "The Rise of Hacktivism and Insider Threats," Symantec, February 17, 2014, http://www.slideshare.net/NortonSecuredUK/symantec-the-rise-of-hacktivism-and-insider-threats.

[35] "Millennials Will Become the Majority in the Workforce In 2015. Is Your Company Ready?," Fast Company, accessed February 4, 2015, http://www.fastcoexist.com/3037823/Millennials-will-become-the-majority-in-the-workforce-in-2015-is-your-company-ready; Rob Asghar, "What Millennials Want in the Workplace (and Why You Should Start Giving it to Them)," *Forbes*, January 13, 2014, http://www.forbes.com/sites/robasghar/2014/01/13/what-millennials-want-in-the-workplace-and-why-you-should-start-giving-it-to-them/; Dan Schawbel, "Why You Can't Ignore Millennials," *Forbes*, September 4, 2013, http://www.forbes.com/sites/danschawbel/2013/09/04/why-you-cant-ignore-Millennials/; Richard Fry, "Millennials Surpass Gen Xers as the Largest Generation in U.S. Labor Force" (Washington, DC: Pew Research Center, 2015), http://www.pewresearch.org/fact-tank/2015/05/11/Millennials-surpass-gen-xers-as-the-largest-generation-in-u-s-labor-force/.

homeland security enterprise must fully understand the risks and implement a suitable mitigation strategy.[36]

C. RESEARCH QUESTION

Leaks and other purposeful secrecy breaches are increasingly common, and the volume of compromised data is growing as well.[37] For the most part, culprits like Snowden believe they have a moral imperative to expose a government that oversteps its authority behind a thick cloak of classification. This viewpoint is becoming more mainstream, starting with the tech-savvy 20- and 30-somethings possessing upwardly mobile potential, but also with very different notions of a good life and good citizenship than their parents espoused.[38] It is becoming its own challenge to (and within) the homeland security enterprise. Homeland security experts have begun to explore the phenomenon of leaks and other insider threats emerging from the up-and-comers in enterprise.

By applying the insider threat risk factors identified by the United States Computer Emergency Readiness Team (US-CERT) to the BabyBoomer, GenX, and Millennial generations, or cohorts, this thesis asks if the generation of "Millennials" is collectively more likely to exhibit the characteristics and traits of an insider threat and ultimately act in a similar manner than previous generations.

---

[36] Chloe Green, "Knowledge Is Power, Data Is Money," Information Age, December 4, 2014, http://www.information-age.com/industry/uk-industry/123458725/knowledge-power-data-money.

[37] According to Symantec's Internet Security Threat Report 2014, the total number of breaches in 2013 was 62 percent greater than in 2012. "Symantec's Internet Security Threat Report 2014," accessed January 3, 2015, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[38] Claude Brickell, "Why Millennials Actually Support Edward Snowden (Whether They Know it or Not), Thought Catalog, July 17, 2014, http://thoughtcatalog.com/claude-brickell/2014/07/why-Millennials-actually-support-edward-snowden/.

D. LITERATURE REVIEW

This literature review is focused on two principles. The first element is the insider threat. The second is the generational cohorts being examined and their associated profiles. The literature available on the subject of insider threats relative to cyber security is mostly from websites, media reports, articles, and seminars; the scholarly examination of this topic is sparse and preliminary. While literature regarding generational cohorts is available in multiple disciplines, all of the disciplines examined agree with and repeat common themes, characteristics, and traits for each group.

1. Who Is an "Insider" and What Is the Threat?

For the purpose of this study, the definition of an insider threat is "people who maliciously and deliberately used their access to cause harm." This definition is an aggregate of several definitions because literature on the subject reveals that, while there are some commonly accepted concepts, there are no clear-cut and universally accepted definitions of an "insider threat." For example, US-CERT and the National Cybersecurity and Communications Integration Center (NCCIC) under the Department of Homeland Security (DHS) define an insider threat as "a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."[39]

The National Insider Threat Task Force Mission Fact Sheet (NITTFMFS) defines an insider threat as "a threat posed to U.S. national security by someone who misuses or betrays, wittingly or unwittingly, his or her authorized access to any U.S. government resource. This threat can include damage through espionage, terrorism, sabotage, unauthorized disclosure of national security

[39] National Cybersecurity and Communications Integration Center, *Combating the Insider Threat* (Washington, DC: U.S. Department of Homeland Security, 2014), https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat.pdf.

information, or through the loss or degradation of departmental resources or capabilities."[40] Similarly, the Office of the Director of Intelligence (ODNI), the government's executive agency with insider threat oversight, defines it as "a person with authorized access to U.S. government resources, to include personnel, facilities, information, equipment, networks, and systems, uses that access to harm the security of the United States. Malicious insiders can inflict incalculable damage. They enable the enemy to plant boots behind our lines and can compromise our nation's most important endeavors."[41] SANS Institute, a well-known non-government organization specializing in information technology security, simplifies the definition. It states insiders are "people who maliciously and deliberately used their access to cause harm."[42]

Although these definitions are similar, there are several important differences. The NCCIC and US-CERT definitions are more broadly focused to include both private and public sector, where the ODNI makes a point to give a government-centric focus to their definition, implying that the insider has access to "U.S. government resources" and is able to "harm the security of the United States." This restriction seemingly implies that compromised private-sector companies either are not victims of insider threats actions or that all insider attacks, regardless of sector, entail an element of harming the "security of the United States." On the other hand, SANS seems to take a more holistic approach, neither specifying who the people are or what they might harm.

Significantly, the NITTFMFS definition includes anyone who acts "wittingly or unwittingly" to reveal insider information. The other organizations not only fail to mention the idea of the unintentional action; they specifically identify the insider as malicious—"intentionally "exceeding" or "misusing" (US-CERT) his or

[40] "National Insider Threat Task Force Mission Fact Sheet," Office of the Director of National Intelligence, accessed August 31, 2013 http://www.ncix.gov/nittf/docs/National_Insider_Threat_Task_Force_Fact_Sheet.pdf.

[41] Ibid.

[42] Eric Cole, *Insider Threats in Law Enforcement* (Bethesda, MD: SANS Institute, 2014), http://www.sans.org/reading-room/whitepapers/analyst/insider-threats-law-enforcement-35402.

her position to ill-intended ends, “maliciously and deliberately” (SANS), inflicting “incalculable damage” (ODNI).[43]

Although malicious and unintentional insiders both pose threats to U.S. security, this study focuses specifically on the malicious insider and the impact membership in a specific group might have on one’s likelihood to compromise information systems.

2. Generations: What’s in a Name?

The population today may be broken into four broad generations: Traditionals, BabyBoomers, GenXers, and Millennials. Demographically speaking, the latter three groups represent the overwhelming majority of the current workforce and thus have the potential to become insider threats. The three generations view the world very differently, and these differences are relevant to the present analysis. Although it is not a significant matter within the confines of this thesis, generally speaking, the parents of the Millennial generation are GenXers who, in turn, are the children of the BabyBoomers.

The U.S. Census Bureau formally recognizes only the term “BabyBoomer,” referring to individuals born in the United States between mid-1946 and mid-1964, during the steady economic growth of the post-World War II decades.[44] Post-war abundance and the era’s social conservatism meant that the Boomers tended to be born to traditionally minded parents who were driven to ensure that their children never experienced the hardships of the Depression, as they had growing up. The hallmarks of the BabyBoomer generation are hopefulness, exploration, and accomplishment. While some Boomers

[43] National Cybersecurity and Communications Integration Center, *Combating the Insider Threat* (Washington, DC: U.S. Department of Homeland Security, 2014), https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat.pdf.; Cole, *Insider Threats*;"National Insider Threat Task Force Mission Fact Sheet," Office of the Director of National Intelligence, accessed August 31, 2013, http://www.ncix.gov/nittf/docs/National_Insider_Threat_Task_Force_Fact_Sheet.pdf.

[44] Sandra L. Colby and Jennifer M. Ortman, *The Baby Boom Cohort in the United States: 2012 to 2060* (P25-1141) (Washington, DC: United States Census Bureau, 2014), http://www.census.gov/prod/2014pubs/p25-1141.pdf.

experimented with the “counter-culture” in their youth, they have since become dominant in the main stream, if only by sheer force of numbers. Many prominent figures in business and entertainment, as well as the most influential people in politics today, hail from this group. Today, Boomers form 39.8 percent of the workforce,[45] but they are retiring at a rate estimated to be nearly 10,000 per day for the next 15 years.[46] Thus, this generation poses less of a threat to industry and government each day.

After the BabyBoomers, there is less clarity about follow-on generations—though most observers at least agree that two distinct cohorts have emerged. The so-called Generation X (GenX), a term introduced into the vernacular in 1992 to distinguish this group from the long-named and well-studied BabyBoomers,[47] encompasses between 44 million and 50 million Americans born from 1965 through early 1980s.[48] These years were characterized by a sharply lower birth rate than during the BabyBoom, and saw the creation of “latchkey” kids as divorce rates increased and working moms became more prevalent.[49] Among general characteristics and traits attributed to GenX are an acceptance of diversity, a practical and pragmatic overview of life, and self-reliance.[50] The GenX tends to comprise multitasking individuals who are technologically savvier than previous generations.[51] In addition, this generation

[45] Matthew Boesler, “Here’s What’s Really Going on with Baby Boomers and the Labor Force,” Business Insider, February 24, 2015, http://www.businessinsider.com/baby-boomers-are-retiring-2014-2.

[46] D’vera Cohn, and Paul Taylor, “Baby Boomers Approach 65 – Glumly,” Pew Research Center, December 20, 2010, http://www.pewsocialtrends.org/2010/12/20/baby-boomers-approach-65-glumly/.

[47] William Strauss and Neil Howe, *Generations*: *The History of America's Future, 1584 to 2069* (New York: Quill, 1991).

[48] “Demographic Profile America’s Gen X,” MetLife Mature Market Institute, accessed February 7, 2015, https://www.metlife.com/assets/cao/mmi/publications/Profiles/mmi-gen-x-demographic-profile.pdf.

[49] Diane Thiefoldt and Devon Scheef, “Generation X and the Millennials: What You Need to Know about Mentoring the New Generations,” Law Practice Today, August 2004, http://apps.americanbar.org/lpm/lpt/articles/mgt08044.html.

[50] Cohn and Taylor, “Baby Boomers Approach 65.”

[51] Ibid.

observes more institutional mistrust than previous generations, perhaps for having grown up amid losing political conflicts and impeached presidents.[52]

Millennials were born from the early 1980s through the early 2000s and, according to Pew Research, are expected to overtake BabyBoomers as the nation's largest living generation by the end of 2015.[53] Michael A. Olguin, who specializes in managing Millennial employees, confirms, "By most definitions, Millennials were born between 1982 and 1996."[54] Another article by human resources expert Susan M. Heathfield says that Millennials "are employees born between 1980 and 2000, or 1981 and 1999."[55] Regardless of a few years' difference, some widely accepted characteristics among the group are the need for structure, leadership, and specific guidance and the demand to be heard.[56] Millennials "have been the subject of endless stories about their racial diversity, their political and social liberalism, their voracious technology use, and their grim economic circumstances."[57]

Furthermore, Millennials are very comfortable working within a team and they have a far higher technology literacy level than previous generations.[58] As a

[52] "Gen-X Is Getting Older," Cornerstone Business Solutions, accessed February 7, 2015, http://www.cornerstoneresults.com/RefLib/KnlgeBk/mrkt_mr_gen-x_is_getting_older.htm.; Value Options, "Baby Boomer Characteristics." Accessed June 16, 2015. http://www.valueoptions.com/spotlight_YIW/baby_boomers.htm..

[53] Richard Fry, "This Year, Millennials Will Overtake Baby Boomers," Pew Research Center, January 16, 2015, http://www.pewresearch.org/fact-tank/2015/01/16/this-year-Millennials-will-overtake-baby-boomers/.

[54] Michael A. Olguin, "5 Tips for Managing Millennial Employees," Inc., April 13, 2012, http://www.inc.com/michael-olguin/5-tips-for-managing-Millennial-employees.html.

[55] "11 Tips for Managing Millennials," About.com, accessed January 1, 2015, http://humanresources.about.com/od/managementtips/a/millenials.htm.

[56] "How to Lead the Millennial," accessed February 7, 2015, http://www.primeast.com/news/how-lead-Millennial.

[57] Paul Taylor and George Gao, "Generation X: America's Neglected 'Middle Child'," Pew Research Center, June 5, 2014, http://www.pewresearch.org/fact-tank/2014/06/05/generation-x-americas-neglected-middle-child/.

[58] "11 Tips for Managing Millennials," About.com.

group, they desire a fun, employee-centered workplace,[59] and this cohort seems less inclined than its predecessors to put in long, tedious hours just to climb the professional ladder; rather, they "expect to be active and engaged parents, which means having the time to parent."[60] They need positive affirmation on a regular basis to feel like they are contributing; they like to have ownership of their work, yet do not respond well when not provided specific guidance.[61]

Millennials, like all generations, are shaped by the times in which they mature. They have always had 'round-the-clock news channels broadcasting graphic images of world events and political bickering.[62] They have learned instant gratification; with a few clicks they can watch their favorite shows at their convenience, rather than on the fixed schedule of a pre-Internet TV network. Online, grassroots political activities are the norm. With technological advances, their world is far more multicultural and focused on globalism, even constantly connected by compact, pocket-size smartphones. They receive lavish praise from their parents and coaches, often receiving trophies simply for participation.

Some of Millennials' defining life moments are the 9/11 World Trade Center attacks and the ensuing wars in Iraq and Afghanistan, the Boxer Day Tsunami in Southeast Asia, and the social media boom.[63] Is it safe to say that

---

[59] Carl Moore, "Fun, Fun, Fun - Millennials Want to Have Fun at Work," *Forbes*, February 28, 2013, http://www.forbes.com/sites/karlmoore/2013/02/28/fun-fun-fun-young-people-want-to-have-fun-at-work/.

[60] Lauren Stiller Rikleen, "How the 'Millennial' Generation Works," American Bar Association, accessed February 15, 2015, http://www.americanbar.org/publications/young_lawyer_home/young_lawyer_archive/yld_tyl_may08_rikleen.html.; Sabrina Franconeri and Joe Maguire, "Associate Evaluations...the Next Generation," *Law Practice Today* (April 2013), http://www.americanbar.org/content/dam/aba/publications/law_practice_today/associate-evaluations-the-next-generation.authcheckdam.pdf.

[61] Olguin,"5 Tips"; Elise R. Zeiger, "Millennials Need Fun, Flexibility at Work," CNN, July 20, 2011, http://www.cnn.com/2011/LIVING/07/20/hot.schedules.millenials/.

[62] "Sensitivity to Criticism," Good Therapy, accessed February 15, 2015, http://www.aei.org/publication/the-events-that-have-shaped-the-Millennial-era/.

[63] Claire Raines, "Generations at Work: Human Resource Management, Generation and Diversity, Generation Definition," accessed February 9, 2015; "The 'Trophy Kids' Go to Work," accessed February 9, 2015, http://www.wsj.com/articles/SB122455219391652725; Robert Tanner, "15 Influential Events That Shaped Generation Y," Management Is a Journey, accessed February 15, 2015, http://managementisajourney.com/15-influential-events-that-shaped-generation-y-infographic/.

they feel a responsibility toward globalism rather than a divided government that cannot agree on simple matters? Should it be a surprise if they use technology to share with the world that which they believe should be shared to make it a better place? And should it come as a surprise that they expect praise for those actions?

E. METHODOLOGY

This thesis hypothesizes that one generation, specifically Millennials, may be more prone to becoming an insider threat than the GenX and BabyBoomer generations, which, along with Millennials, comprise 95 percent of today's workforce.[64] It accomplishes this by comparing the generations against known insider threat risk factors and identifying which generation demonstrates the most indicators.

Using individual markers that influence individuals'' actions (such as past and present socio-economic circumstances, education levels, and occupational position) makes it possible to identify a specific individual as a potential or elevated threat. While these markers are certainly related to the insider threat question and the influences on an *individual* to become a threat, these markers would be present across all the generations in significant numbers. Thus, analyzing the generations based on the individual, then by extension assigning the determination of the individual as representative of the generation, would be meaningless. For this reason, the research for this thesis examines each generational cohort as a whole rather than studying any specific or arbitrary subset of random individuals within the generations, then makes broad categorizations of the entire group based on selective case studies.

The data sources utilized for this study stem from a variety of functional areas, disciplines, and organizations. Insiders' motivations are gathered through various behavioral analysis entities such as US-CERT, the Federal Bureau of

[64] The traditional generation, born before 1945, represents 5 percent of the U.S. workforce as of 2012. That percentage continues to shrink as those workers exit the workforce. http://www.catalyst.org/knowledge/generations-workplace-united-states-canada 22 Jul

Investigation (FBI), Department of Defense's Personnel and Security Research Center (PERSEREC) and published, first-hand accounts and descriptions of known insiders and those who encourage them. Additionally, results from various sources, such as personality type and indicator tests, and psychological studies are analyzed for generational patterns.

Data collected and used for this study enumerating successful insider threat compromises was provided by Carnegie Mellon's Computer Emergency Response Team (CERT). This data has been collected and tabulated since 1996 to capture a variety of data points about successful insider threat attacks. While there are a number of information technology (IT) security companies, like Vormetric, Symantec, and RSA, that collect data from organizations willing to volunteer it as it relates to successful compromises, CERT is the only organization with no financial or other vested interest in collecting and presenting the data in a manner beneficial to their organization. This independence adds to the credibility and bias-free aspect of their data.

The database managed by CERT has a number of data fields; however, the only fields that were relevant and therefore used within this study were the insider's age at the time of the attack, the year during which the attack began, and the industry and type of attack. The age and year were used to determine the attacker's generational. The sector and type of attack were included to demonstrate that insider threats use a variety of tactics and operate in a wide array of industries, underscoring the importance of cyber diligence for all businesses.

The methodology used for this study was first to examine the 14 relevant critical factors indicative of an elevated probability for becoming an insider threat. Then, using reliable references and sources—some of which are law enforcement, academic, and cyber security-related—factors were applied to relevant cohorts. The intent was not to assign each factor to only a single cohort in a one to one relationship based on which cohort has the strongest claim to a given factor. Rather, it was to assign each factor to as many or as few concurrent

cohorts as the analysis deemed appropriate. In the end, only five of the fourteen factors applied to a single cohort, the remaining nine factors were found to apply to multiple cohorts.

Once factors were assigned to the cohorts, the cohorts were ranked based on the total number of attributed indicators. The cohort with the highest number of attributed factors was designated as the most likely to become an insider threat. At this point, based on the analysis, it was determined whether the Millennial generation collectively possesses more precursors than other generations in the workforce today and, therefore, is more likely to become an insider threat.

With the CERT data on hand, however, it was then possible to validate the findings based on actual data. The validation was determined by analyzing the representative population of the generation in any given year and deriving the percentage of compromises perpetrated by the generation. After aggregating the annual data, it showed, independent of the hypothesis prediction, which of the generations is the one that has committed the most compromises, thereby confirming or refuting the analysis. This analysis provides input for future decision makers or a baseline from which future researchers can further investigate the hypothesis.

This study can help organizations build proactive systems and mitigation efforts to respond to possible insider threats. If the data provides sufficient evidence so that the theory appears to be true, it will provide input to policy makers when considering strategic directions of insider threat risk reduction. Because 50 percent of the workforce will be comprised of Millennials by 2020, and they may be more likely to conduct insider-threat behaviors, organizations can allocate resources commensurate with the threat. If the data does not sufficiently support the theory that Millennials pose a greater threat, these same policymakers can practice risk-based defensive measures by reducing expenditures toward an area where there is less probability of a threat. These

resources can then be reallocated elsewhere to strengthen the overall security of the enterprise.

F. CHAPTER OVERVIEW

Chapter II develops the insider threat concept, defining the term's elements and discussing the insider's motivations. It then introduces the risk factors used throughout the remainder of the thesis. Chapter III examines the generational cohorts and establishes the risk factors prevalent with the specific cohort, studying the statistics behind insider threat attacks, looking at the cohort as a percentage of the workforce, and extrapolating the pro-rata percentage of the attacks against each cohort. Chapter IV examines data gathered from cyber security organizations. This data provides validation of the findings in Chapter III, allowing the theoretical answer to the thesis question to be compared against actual historical data. Chapter V concludes the thesis with a summary of the results, punctuated with a critical analysis of the study.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE INSIDER THREAT

This chapter discusses the idea of an insider threat, including a working definition of the term. It also reveals that the definition varies somewhat based on the defining organization and sector (private versus public). The chapter also discusses common motivations that cause individuals to engage in what are ultimately illegal acts

Once this background is established, the chapter introduces the fourteen factors used to analyze the generations, ranks them from strongest to weakest influence, and then breaks down each factor's meaning. The factors discussed are irrational ones, in a sense that the individual, or in this study a generation, may possess these factors without self-awareness in their rational, or cognitive, behaviors. As such, these characteristics are difficult to repress or subdue, providing a valuable gauge by which to analyze the generations. US-CERT, an authoritative source regarding cyber security and defenses, identifies these factors as characteristics indicative of insider threat potential.[65]

A. DEFINITIONS

There are two elements to defining an insider threat. The first requires understanding who is considered an insider; the second is understanding the idea of a threat. First, who or what is an "insider?" Unfortunately, the only clear-cut element in defining an insider is that there is no clear-cut way to define an insider. Regardless of the definitions' inconsistencies—whether an insider requires access specific to only government systems or private sector as well, intentional or unintentional access, or to do harm to the United States or just the private-sector employer—the one constant in defining an insider is that it is a person within an organization who abuses his or her access.

[65] National Cybersecurity and Communications Integration Center, *Combating the Insider Threat*.

An insider becomes a "threat," according to the National Cybersecurity and Communications Integration Center (NCCIC), when the individual uses his or her authorized access, wittingly or unwittingly, to do harm.[66] Whether that harm is to the security of the United States or the profits of a company are somewhat irrelevant in this context. The main emphasis in this study is whether Millennials, working either in the private or public sector, are more likely to abuse their trusted access than members of a different generation.

The private-versus-public-sector differentiation in many disciplines might well be an important and distinct difference; for this thesis, however, there is no distinction, as the study is focused on the Millennial, BabyBoomer and GenX generational attributes at large. While perpetrators' intentions and data sensitivity may vary among breached institutions in both sectors, the focus of this study is a person (or group of persons') broader inclination to abuse insider status to leak or obtain information unlawfully.

B. MOTIVATION

In the cyber-security realm, there is a common tenet referred to as the "C-I-A Triad," which stands for confidentiality, integrity, and availability—the goals of any cyber-security program. Confidentiality means that only those who should have access to view data can, in fact, view the data. Integrity means the data used is in its original, intended form. Availability denotes that the data is ready to be accessed when the user or system calls for it. A breach of any one of these three areas would be considered a security event, regardless of the compromiser's intentions.

As an example, someone who somehow accesses data they are not permitted to access has committed a security breach. There are varying factors

[66] "The National Cybersecurity and Communications Integration Center (NCCIC) is an element within the Department of Homeland Security and is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the federal government, intelligence community, and law enforcement." "About the National Cybersecurity Integration Center," Department of Homeland Security, accessed August 25, 2015, http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.

concerning this example (i.e., if the individual actually copied the data and removed it from the premises, or simply read it) but information security does not differentiate between the two in defining them as security events. Organizational policies determine what kind of action should be taken against the individual, based on what was done with the data.

In a study on insider threats conducted by Cisco Systems, it was found that 99 percent of end users in the United States have never violated their organizational trust by accessing data that they were not permitted to access.[67] Three percent, however, stated they have "known someone at work who has accessed someone else's computer to look for unauthorized personal or corporate information."[68] So what would motivate an otherwise benign employee to compromise organizational data? The Defense Personnel and Security Research Center (PERSEREC) states that motivation is the "result of a complex interaction between personality characteristics and situational factors."[69]

Given the right combination of personal and professional influences—anything from being passed over for a promotion to not receiving praise, to even feeling dissatisfied with the government—the irrational processes can cause an otherwise rational person to betray the trust of his or her workplace. Richards J. Heuer, Jr., a researcher with PERSEREC, argues that "it depends only upon an insider with the opportunity to betray, some combination of character weaknesses and situational stresses, and a trigger that sets the betrayal in motion."[70] While there are countless factors that may motivate people to betray that trust, some of the more common factors include financial burden; the

[67] Cisco Systems, Inc. is an American multinational technology company that designs, manufactures, and sells networking equipment.

[68] Cisco*. Data Leakage Worldwide White Paper: The High Cost of Insider Threats* (C11-506224-00) (San Jose, CA: Cisco Systems, 2008), http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.pdf.

[69] "Opportunities and Motivation Are Increasing," Defense Human Resources Activity, accessed June 15, 2015. http://www.dhra.mil/perserec/osg/counterintelligence/opportunity-motive.htm#Increasing%20Opportunity.

[70] Richards J. Heuer, "Insider Espionage Threat," U.S. Department of Agriculture, accessed August 18, 2015, http://www.dm.usda.gov/ohsec/pdsd/Security%20Guide/Treason/Insider.

perception of being treated unfairly by an employer; misguided ideas regarding patriotism leading to feelings of loyalty to a foreign country or to a global community;[71] or a desire to cause shame or embarrassment to the organization, agency, administration or country.[72]

Two primary motivation factors, however, are profit and revenge.[73] The motivation of profit is simple: the insider is merely seeking financial gain. The attractiveness of quick wealth can provide significant temptation, especially to lower-ranking, lower-paid employees with access to sensitive data. With the valuable data available to these employees, especially those working within the homeland security enterprise, providing data to a foreign country, drug cartel, terrorist organization or organized crime syndicate could mean easy money.

One example of a financially-motivated insider is Wen Chyu Liu, a retired research scientist from Dow Chemical. In February 2011, Liu was convicted on one count of conspiracy to commit trade secret theft and one count of perjury, stemming from his role in stealing trade secrets from his former employer and selling them to companies in China. Liu attempted to sell the data while he traveled around China, paid Dow Chemical employees, both past and present, for products and information, and bribed an employee to provide documents.[74] In January 2012, he received a sentence of five years in federal prison. In addition, Liu also received two years of supervised release, was fined $25,000, and was ordered to forfeit $600,000 by the federal jury.[75]

Revenge is an equally comprehensible motivator. The insider seeks retribution for some type of action, either real or perceived, against the

[71] "'Edward Snowden Is a Patriot': Ex-NSA CIA, FBI and Justice Whistleblowers Meet Leaker in Moscow," Democracy Now!, October 14, 2013, http://www.democracynow.org/2013/10/14/edward_snowden_is_a_patriot_ex.

[72] Ibid.

[73] Shelley A. Kirkpatrick, "Refining Insider Threat Profiles," *Security* 45, no. 9 (September 2008): 56, 58, 60, 62–63.

[74] The Insider Threat," FBI, accessed June 15, 2015, https://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure.

[75] Ibid.

organization responsible for that action. An insider wishing revenge, however, does not necessarily need to steal data. Instead, the malicious insider may simply corrupt the data or cause harm to the information system, which, if the insider possesses sufficient technical skills, could be difficult or nearly impossible to detect. The fact that Snowden was able to remove, without being detected, all the classified data that he did with just thumb drives is enough to show that even top security measures can be defeated with relative ease given a highly motivated individual.

C. US-CERT RISK FACTORS

What possesses a person to become "unjust," to act in a manner that is contrariety to social norms? Snowden. Manning. Hanssen. Ames: these names represent many things to many people—betrayal, deception, and treachery, to name a few. Whatever thoughts these individuals evoke, there is one underlying element in all their actions. Each one of them made a decision in which the inherent risks were worth the consequences associated with getting caught.

US-CERT has identified 14 characteristics that increase a person's risk of becoming an insider threat[76]; they are listed here according to their relative importance in an effort to assign a weight to each for the final analysis. The importance was determined by carefully examining each factor and estimating which would have the strongest negative influence to the weakest negative influence. The factors, as defined US-CERT and in order from strongest to weakest negative influence, are:

- greed/financial need
- entitlement—narcissism (ego/self-image)
- ethical "flexibility"
- vulnerability to blackmail

[76] US-CERT is an organization within the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD). It is accepted among cyber security practitioners as an authoritative agency relative to all elements of cyber security and defenses.

- reduced loyalty
- rebelliousness, passive aggressiveness
- compulsive and destructive behavior
- introversion
- lack of empathy
- predisposition toward law enforcement (authority)
- minimization of mistakes or faults
- intolerance of criticism
- inability to assume responsibility for actions
- self-perceived value exceeds performance[77]

These characteristics are the main thread used throughout this paper to determine if Millennials are collectively more likely to exhibit the characteristics and traits of insider threats. With this in mind, what indicators (psychological, behavioral, or otherwise) might alert others to an individual's possession of these fourteen characteristics? In the next section, this question is examined.

D. CHARACTERISTIC ANALYSIS

(1) Greed/Financial Need

Greed is defined in *Psychology Today* as "the excessive desire for more than is needed or deserved, not for the greater good but for one's own selfish interest, and at the detriment of others and society at large."[78] While greed may lead to economic success, it is generally not seen as a positive personal characteristic. Greed is also an element in any addiction; the addict never has enough (whether it be drugs, alcohol, gambling, or sex). For the malicious insider, the addict never has enough money. As Dr. Leon F. Seltzer explains,

[77] National Cybersecurity and Communications Integration Center, *Combating the Insider Threat*.

[78] Neel Burton, "Is Greed Good?: The Psychology and Philosophy of Greed," *Psychology Today*, October 6, 2014, https://www.psychologytoday.com/blog/hide-and-seek/201410/is-greed-good.

"Ask a multi-millionaire or billionaire so afflicted (if you can find one willing to talk to you!), and you'll discover that their 'mega fortune quest' really has no end point. They won't be able to name the definitive 'millionth' or 'billionth' that, finally, will do it for them. They can't because the means by which they reap their riches has *itself* become the end."[79] As the addict sinks deeper into addiction, he or she seeks more and more of the object of addiction—in this instance, money.

Greed can indicate a malicious insider's desire to place wealth and material objects above ideals of right and wrong, or loyalty to an organization or even a country, especially if the accessible information has value to another organization.

(2) Introversion

An introvert is defined as "a person who is focused on (often preoccupied) with his or her private mental experiences, feelings, and thoughts. The term was developed by Carl Jung in his theory of personality."[80] Introverts tend to be quieter, reserved, and introspective, and introversion is one of the major personality traits in the "big five" dimensions of personality.[81] Social situations will cause an introvert to expend energy, unlike extroverts, who get increased energy from social interactions. An introvert will often need to spend time alone to rejuvenate following a social event or spending time with a large group of people.

There are several traits that are associated with introversion. For instance, introverts tend to be detail oriented, thoughtful and self-aware; they desire more

[79] Leon F Seltzer, "Greed: The Ultimate Addiction," *Psychology Today*, October 17, 2012, https://www.psychologytoday.com/blog/evolution-the-self/201210/greed-the-ultimate-addiction.

[80] "Introvert (Introversion)," Psychology Glossary, accessed September 2, 2015, http://www.alleydog.com/glossary/definition.php?term=Introvert%20(Introversion).

[81] "Today, many researchers believe that there are five core personality traits. Evidence of this theory has been growing over the past 50 years, beginning with the research of D. W. Fiske (1949) and later expanded upon by other researchers including Norman (1967), Smith (1967), Goldberg (1981), and McCrae & Costa (1987). The 'big five' are broad categories of personality traits. While there is a significant body of literature supporting this five-factor model of personality, researchers don't always agree on the exact labels for each dimension." See Kendra Cherry, "What Are the Five Major Personality Traits?," accessed July 16, 2015, http://psychology.about.com/od/personalitydevelopment/a/bigfive.htm.

self-knowledge and self-understanding than knowledge and understanding of others. Introverts are commonly quiet and reserved in a large group or around unfamiliar people, keeping their emotions to themselves; but when around people they know well, however, they will be more social and outgoing.

An introverted malicious insider would seek jobs with little social interaction, choosing careers that involve working independently.

(3) Vulnerability to Blackmail

Blackmail is a threat conveyed from one person (the blackmailer), who typically has information, to another person (the victim), who wishes that information to remain secret. The blackmailer can leverage the victim's job, reputation, or even a spouse, or threaten to expose a victim's committed crime, immoral activity, or wrongdoing. While this is a behavioral (as opposed to a psychological) characteristic, the actions that make one susceptible to blackmail—such as excessive alcoholism, promiscuity, or criminal activity—may be rooted in psychological influences during developmental stages of life.[82] The victim often complies with the blackmailer out of fear.[83]

Blackmail susceptibility has been used in conjunction with other factors to motivate a malicious insider. As an example, Aldrich Ames initially intended only to provide the Soviets with "worthless" information for $50,000 to cover his debts, but once he crossed that line he wanted more (greed), and the KGB's blackmail threats kept him betraying his country for years.[84]

(4) Compulsive and Destructive Behavior

According to *Psychology Today*, a compulsive person is one who is "trapped in a pattern of repetitive and senseless thinking—and these behaviors

[82] Jed Shlackman, "Psychology, Spirituality, and the Manipulation of Human Society," Examiner, June 9, 2013, http://www.examiner.com/article/psychology-spirituality-and-the-manipulation-of-human-society.

[83] Ibid.

[84] "Aldrich Ames," Wikipedia, last modified 17 August 2015. http://en.wikipedia.org/wiki/Aldrich_Ames

can prove quite difficult to overcome."[85] Other definitions expand on that notion, adding that the behavior may not necessarily result in actual reward or pleasure. Compulsive behavior…"is usually a small, restricted and repetitive behavior, yet not disturbing in a pathological way. Compulsive behaviors are a need to reduce apprehension caused by internal feelings a person wants to abstain or control."[86] There are a number of ways that a person can display destructive behavior, for example "overeating, nail-biting, hoarding, gambling and lying."[87]

Destructive behavior or (self-destructive behavior) is a conceptual phrase that describes collections of actions taken by an individual leading to abuse or harm, whether to one's self, or to other people or property. The behavior stems from individuals not liking or loving themselves wholly. People with eating disorders, for example, may like or love their level of education, but they might not like of love their weight. Or a person might constantly put others down because he does not like where he sees himself, so, in an attempt to boost self-esteem, he tries to bring others down to his perceived level.[88]

According to a LiveScience report from 2011, the 10 biggest (self-) destructive behaviors (and, as such, behaviors to watch for in countering the insider threat) are lying, craving violence, stealing, cheating, clinging to bad habits, bullying, cosmetic surgery and tattoos/piercing, stressing out, gambling, and gossiping.[89] These behaviors are visible in all walks of life and transcend socioeconomic barriers: the Hollywood actors and actresses like the late Joan Rivers and Mickey Rourke who seek the surgeon's knife to keep a youthful

[85] "Compulsive Behaviors," *Psychology Today*, accessed August 18, 2015, https://www.psychologytoday.com/basics/compulsive-behaviors.

[86] "Compulsive Behavior," Freebase, accessed August 18, 2015, https://www.freebase.com/m/0281lfw.

[87] "Compulsive Behaviors," *Psychology Today*, accessed August 18, 2015, https://www.psychologytoday.com/basics/compulsive-behaviors.

[88] "Understanding the 10 Most Destructive Human Behaviors," Live Science, May 13, 2011. http://www.livescience.com/14152-destructive-human-behaviors-bad-habits.html.

[89] Ibid.

appearance; the inner-city youth who seem committed to violence; the adolescent self-expressionists who crave tattoos and body piercings.

(5) Rebelliousness, Passive Aggressiveness

According to *Psychology Today*, passive aggressiveness is "a deliberate and masked way of expressing covert feelings of anger"[90] and "may stem from specific childhood stimulus," after which the child was never free to express frustration or anger.[91] Passive aggressiveness is demonstrated by passive resistance to expected behavior, be it work, school, or other social norms. Being passive aggressive is a way for one person to "get back" at another without the other person necessarily recognizing the anger.

Examples of passive aggressiveness can be difficult to identify initially. The trait can manifest in a variety of ways, such as an individual intentionally making mistakes. Rather than saying no to a request, the individual performs poorly, hoping the substandard performance will prevent a future request of a similar nature. A passive aggressive person may also want the last word in disagreements, often even when the disagreement has been sorted out. Some other common passive aggressive behaviors include: procrastination; behaving contrary to social norms; ignoring, or pretending to ignore, others; overtly not talking to someone; moping; and gossiping.[92]

[90] Signe Whitson, "10 Things Passive Aggressive People Say," *Psychology Today*, accessed August 18, 2015, https://www.psychologytoday.com/blog/passive-aggressive-diaries/201011/10-things-passive-aggressive-people-say.

[91] Jeffrey G. Johnson et al., "Childhood Maltreatment Increases Risk for Personality Disorders during Early Adulthood," *Archives of Psychiatry* 56, no. 7 (July 1999): 600–6.

[92] "8 Examples of Passive Aggressive Behaviour," Coaching Positive Performance, accessed August 18, 2015, http://www.coachingpositiveperformance.com/8-examples-passive-aggressive-behaviour/.

(6) Ethical "Flexibility"

Ethics "involves systematizing, defending, and recommending concepts of right and wrong behavior."[93] Such right or wrong behavior could include policy adherence, regardless of one's personal belief in the policy, and maintaining honesty and integrity in the workplace.

An individual with flexible ethics, given the right rationalization, would allow a situation to dictate his or ethics rather than having steadfast internal ethics dictate personal actions. Such a characteristic could well lead to other situations, similar to Eric Snowden's, in which people convince themselves that their actions are warranted because they are doing something for the greater good.

(7) Reduced Loyalty

To be "loyal," a person is sovereign, "to his or her government or state"[94]—a loyal subject, for instance, is faithful to his "oath, commitments, or obligations"[95] (as in a loyal vow); a loyal follower is "faithful to any leader, party, or cause, or to any person or thing conceived as deserving fidelity"[96] (as in being a loyal friend); or someone with a loyal personality is faithful to commitments,

[93] Ethics varies slightly within professions. As an example, business ethics is defined as "proper business policies and practices regarding potentially controversial issues, such as corporate governance, insider trading, bribery, discrimination, corporate social responsibility and fiduciary responsibilities. Business ethics are often guided by law, while other times provide a basic framework that businesses may choose to follow in order to gain public acceptance." The Americal Medical Association has a Council on Ethical and Judicial Affairs (CEJA) which is made up of "seven practicing physicians, a resident or fellow, and a medical student" to "analyze and address timely ethical issues that confront physicians and the medical profession." Ethics in politics was described in a Harvard paper as "the practice of making moral judgments about political action, and the study of that practice."

[94] "Loyal," Dictionary.com, accessed May 27, 2015, http://dictionary.reference.com/browse/loyal.

[95] Ibid.

[96] Ibid.

vows, allegiance, obligations, etc.[97] Loyalty itself is considered by many to be a virtue and, as such, the mental health profession, which believes virtues are good, considers loyalty to be an indicator of good mental health.[98] As one begins to be less loyal to his government, ignores his oaths, or becomes less faithful allegiances, the person in question would have less hesitation to divulge secrets. With the mental health community saying loyalty is a sign of good mental health, is it safe to say that those who betray their organizations, effectively shunning their loyalty, are in poor mental health?

(8) Entitlement—Narcissism (Ego/Self-Image)

Narcissism manifests itself with "arrogant behavior, a lack of empathy for other people, and a need for admiration—all of which must be consistently evident at work and in relationships."[99] Among narcissists, cockiness tends to make them believe that they are smarter than others and, as such, the likelihood of being caught is minimal. They are often self-centered, manipulative, and demanding, focusing their efforts on "unlikely personal outcomes" such as fame and glory, and may feel that they are entitled to some level of special treatment.[100]

The narcissist is more likely to commit acts damaging to an organization if he or she believes such acts could bring notoriety. Edward Snowden, for example, believed he would not get caught unless on his own terms.

Several of the following characteristics, when present in an individual, could indicate narcissism. These "sub-characteristics" are defined in the following subsections.

---

[97] Ibid.

[98] Michael J. Hurd, "The Psychology of Loyalty (DE Wave)," Living Resources Center, accessed May 27, 2015, https://drhurd.com/the-psychology-of-loyalty-de-wave/.

[99] "Narcissistic Personality Disorder," *Psychology Today*, Last Modified February 17, 2015, https://www.psychologytoday.com/conditions/narcissistic-personality-disorder.

[100] Ibid.; "Narcissistic Personality Disorder Symptoms," Psych Central, accessed May 20, 2015, http://psychcentral.com/disorders/narcissistic-personality-disorder-symptoms/.

Minimizing their mistakes or faults

This characteristic is referred to as minimization, which is "underestimating one's importance and relevance to events."[101] This idea of minimization dovetails with the narcissism previously described. In order make themselves seem better than others, narcissists' faults would have to be downplayed, lest others see the shortfalls as a weakness.

In minimalizing, the individual hopes that his mistakes or faults appear to be trivial, and he is therefore more likely to be accepted or liked by coworkers.[102] Additionally, those who minimize their actions attempt to convince others that the actions are not as detrimental as they truly are. In doing so, the minimizers are attempting to get others to see them in a better light, again dovetailing with the narcissist.

Inability to assume responsibility for their actions

An individual's inability to take ownership for his or her actions is a relatively simple concept and is present in some form in nearly every workplace. This characteristic differs from minimizing mistakes primarily in that the actions in question may or may not be mistakes, per se. As an example, a person might decide to implement a particularly poor course of action, despite opposing advice, which results in negative consequences for an organization. While it is not a mistake in the sense of the definition,[103] it is an action that may require accountability—the accountability a person is unwilling to accept in this characteristic. This minimizer is the person who, regardless of the circumstances, will not own up to his actions. He will lay the blame on anything possible, such as

[101] "What Is Minimization?," Psychology Dictionary, accessed May 25, 2015, http://psychologydictionary.org/minimization/.

[102] George Simon, "Minimization: Trivializing Behavior as a Manipulation Tactic," accessed May 27, 2015, http://counsellingresource.com/features/2009/02/23/minimization-manipulation-tactic/.

[103] As defined by *Merriam Webster's*, a mistake is "to understand (something or someone) incorrectly, to make a wrong judgment about (something), to identify (someone or something) incorrectly." See "Mistake," accessed August 31, 2015, http://www.merriam-webster.com/dictionary/mistake.

a supervisor, subordinates, and lack of personnel, money, or time. This lends itself to the narcissist subcategory because, in a narcissist's mind, he cannot possibly be the reason for any type of failure; accordingly, he will seek out those he deems inferior and, therefore, must be the cause of said failure.

This characteristic is somewhat simpler to identify than others. The person with this attribute would not accept root cause analysis findings pointing to any area for which they are responsible. As an example, system upgrades that fail would be because of hardware incompatibility or possibly a network connectivity issue—not because of the faulty code they wrote, despite abundant contrary evidence.

Intolerance of criticism

While nobody enjoys being criticized, some are completely incapable of handling any sort criticism. The average person, when hearing others' criticisms, can usually filter through it and identify any elements of truthful feedback and process it effectively. Others, however, are incapable of such processing. They cannot maintain any levelheadedness in dealing with the criticism. With a dish-it-out-but-can't-take-it mindset, these people are often very quick to criticize others. Potential warning signs of being overly sensitive to criticism include extreme defensiveness when criticized, "anxiety, depression, anger, shame, or other intensely negative emotions."[104] This trait is also fairly easy to identify. The individual in this case would resist criticism much in the same manner as one unable to assume responsibility for actions, attempting to deflect the root of the criticism to outside influences of simply disregarding it.

On the surface, this characteristic might also sound similar to "inability to assume responsibility for their actions" and "minimizing their mistakes or faults." The primary difference, however is that, unlike the previous two, intolerance of

[104] "Therapy for Sensitivity, Therapist for Sensitivity Issues," accessed May 27, 2015, http://www.goodtherapy.org/therapy-for-sensitivity.html.; Leon F. Seltzer, "The Narcissist's Dilemma: They Can Dish it out, But …," *Psychology Today*, October 12, 2011, https://www.psychologytoday.com/blog/evolution-the-self/201110/the-narcissists-dilemma-they-can-dish-it-out.

criticism may well have nothing to do with a mistake, fault, or action. It may come on the heels of a successful project—for example, during an after-action or lessons-learned session, areas that were less successful than others are discussed. These constructive criticisms then lead to perfectly reasonable discussions regarding better ways of doing a task in the future. An individual with this characteristic would be unable to comprehend the constructive nature of the discussions, instead seeing it as an attack on personal abilities, resulting in defensiveness.

Lack of empathy

Empathy is the ability of a person to comprehend and share the feelings of another person.[105] According to *Psychology Today*, "lack of empathy is one of the most striking features of people with narcissistic personality disorder."[106] "Narcissists do not consider the pain they inflict on others; nor do they give any credence to others' perceptions," says Dr. Les Carter in the book *Enough of You, Let's Talk About Me*; he continues, "They simply do not care about thoughts and feelings that conflict with their own."[107] One should not expect the narcissist to listen to, understand, or show support for another person. To better understand the mindset, consider the words of Sam Vaknin, author and self-proclaimed narcissist: "I am aware of the fact that others have emotions, needs, preferences, and priorities—but I simply can't seem to 'get it into in my mind'…I know how I should feel because I am well-read—but I cannot seem to bring myself to emote and to sympathize."[108]

---

[105] Empathy should not to be confused with idealism, which means "the attitude of a person who believes that it is possible to live according to very high standards of behavior and honesty" and pertains primarily to the self, with no specific regard for others. (http://www.merriam-webster.com/dictionary/idealism)

[106] "Randi Kreger, "Lack of Empathy: The Most Telling Narcissistic Trait," *Psychology Today*, January 24, 2012, https://www.psychologytoday.com/blog/stop-walking-eggshells/201201/lack-empathy-the-most-telling-narcissistic-trait.

[107] Les Carter, *Enough About You, Let's Talk About Me: How to Recognize and Manage the Narcissists in Your Life*, 1st ed. (Jossey-Bass, 2008), 9.

[108] Bianca Smith, "What's in it for Me?," The Fickle Heartbeat, April 26, 2015, http://thefickleheartbeat.com/2015/04/26/whats-in-it-for-me/.

Self-perceived value exceeds performance

When narcissists' "arrogant behavior" and "need for admiration…at work"[109] are coupled with their air of superiority, it stands to reason that they would have an inflated perception of the value they bring to an organization. This characteristic flaw would likely be recognizable by co-workers but, given the narcissists' inability to take criticism constructively, they would not address the issue and let it remain unspoken.

The last of the characteristics is less specific to psychology; rather, they are behavioral patterns and elements of self-opinion. Having a predisposition to law enforcement implies that the predisposition is negative in nature. As such, this behavior would be easily recognizable and may manifest itself in anything from statements disparaging law enforcement officers to actively participating in demonstrations, similar to the ones recently in Ferguson, Missouri and Baltimore, Maryland.[110]

E. CONCLUSION

While the presence of one or more of these characteristics in and of themselves does not guarantee the individual will be a threat, there is enough correlation that would indicate that the presence of these characteristics, especially in increasing quantities with the outside variables introduced, would make a person more likely to betray his or her organization.

In the case of Snowden, his actions display indications of narcissism— he has never placed any of the blame for his actions on himself, rather blaming the NSA for their program, the U.S. State Department for pulling his passport

[109] "Narcissistic Personality Disorder," *Psychology Today*.

[110] Ferguson, Missouri was the scene of two separate violent protests over the actions of the police. Initially, there were riots from August 9 to the 25th following the fatal shooting of Michael Brown by a police officer. The second wave of violent protests occurred from November 24th to December 2nd, following a decision by the grand jury to not indict the officer in the shooting. Violent protests occurred in Baltimore, Maryland from April 18th until May 3rd following the death of Freddie Gray at the hands of six police officers while in custody. The officers have been charged with multiple crimes.

(ultimately leaving him stranded in Russia), and the users who shared their login information with him, allowing him to access files he would otherwise not have been able to access. Whether one considers him a traitor, hero, or a national security threat, his rebelliousness is without question. What he did was an absolute resistance to authority and convention. Further, he displayed a pattern of frustration when his superiors took no actions following his attempts to expose the programs he felt were infringing on liberties of people around the world.

Snowden also showed ethical flexibility. His actions were no doubt unethical and self-serving: stealing; compromising national security; jeopardizing lives. However, the flexibility element is that he believed, regardless of the ethicalness of his actions, he was bringing to light something larger that needed to be leaked. Snowden stated, "I didn't want to change society. I wanted to give society a chance to determine if it should change itself. All I wanted was for the public to be able to have a say in how they are governed."[111]

Thus, Snowden exemplifies four of the fourteen characteristics examined in this thesis, and described by US-CERT as indicators that one might become an insider threat.[112]

This incident, as with many such compromises in cyber security, demonstrates that the factors are easily identified after the fact. The challenge cyber security practitioners face on a daily basis is keeping ahead of the threats by putting the pieces together before a breach happens, ultimately to accomplish cyber security prevention rather than reacting, responding to, and recovering from cyber incidents.

---

[111] Barton Gellman, "Edward Snowden, after Months of NSA Revelations, Says His Mission's Accomplished," *Washington Post*, December 23, 2013, https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html.

[112] The United States Computer Emergency Readiness Team (US-CERT) is an organization within the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD). It is accepted among cyber security practitioners as an authoritative agency relative to all elements of cyber security and defenses.

THIS PAGE INTENTIONALLY LEFT BLANK

III. ANALYSIS

This chapter analyzes the fourteen insider-threat factors and determines which can be applied to particular generational cohorts. Where a factor—for example, greed/financial need—might apply to multiple cohorts, it is assigned and tabulated as such. Tabulating the factors against the cohorts provides the generational threat hierarchy, which helps determine if the Millennials are the cohort most likely to be an insider threat. This sets up the comparison, in Chapter IV, against actual cases of insider threat compromises.

A. DATA ANALYSIS METHODS

Each characteristic is only subscribed to a specific cohort when it can be demonstrated, based on available evidence that the given cohort possesses that characteristic. The final step consists of tabulating the total number of threat characteristics possessed by each cohort to establish the threat hierarchy, which is the cumulative score of each cohort's characteristics.

This hierarchy allows the cohorts to be ordered from most-likely to least-likely insider threat, allowing for a theoretical answer to the thesis question. The cohort that possesses the highest cumulative total of the fourteen characteristics would be the one most likely to produce potential insiders.

B. ESTABLISHING THREAT HIERARCHY

Greed/financial need

Studies have shown that Baby Boomers are considered to be the greediest generation. Contrasting studies, however, contend that Millennials are concerned for themselves and less likely to be generous in their charitable

contributions than the Baby Boomers.[113] Regardless of the varying degrees and discussions concerning the level of greediness, the consensus is that both the generations possess levels of greediness, making both of these cohorts susceptible to the greed characteristic.

Table 1 displays the analysis results, showing whether the specific factor being discussed applies to each generation. Each factor will have a similar table following its analysis, with the individual tables aggregated following the final analysis for a holistic view.

Table 1. Greed/Financial Need Applicability

	Applies to Cohort?		
	BabyBoomers	GenX	Millennials
Greed, financial need	--	--	Yes

The table following each analysis displays which cohort has been shown to possess the analyzed characteristic, indicated by the yellow shading.

Compulsive and destructive behavior

While Boomers tend to use quiet reflection, prayer, and talking with trusted associates to handle stress and anxiety, several studies indicate that anxiety and "disorders such as obsessive-compulsive disorder and panic disorders are higher

[113] "Millennial Generation Money-Obsessed And Less Concerned With Giving Back, Study Finds," Huffington Post, accessed July 5, March 15, 2012, http://www.huffingtonpost.com/2012/03/16/Millennial-generation-study-fame-money_n_1354028.html.; Alexander S. Balkin, "Baby Boomers Ruined America: Why Blaming Millennials Is Misguided—and Annoying," Salon, October 20, 2014, http://www.salon.com/2014/10/20}/baby_boomers_ruined_america_why_blaming_millennials_is_misguided_and_annoying/; Laurence J. Kotlikoff, "Baby Boomers: The Greediest Generation," *Forbes*, November 11, 2010, http://www.forbes.com/2010/11/11/greedy-boomers-social-security-medicare-cuts-personal-finance-kotlikoff.html.

in baby boomers" when compared to other generations.[114] "We know for scertain that baby boomers have a higher prevalence rate of depression than the generation before them,"[115] says Dr. Donald A. Malone, Jr., director of the Mood and Anxiety Clinic in the department of psychiatry and psychology at the Cleveland Clinic. "The fact remains that we are not sure why—but much of the research is pointing to daily stress as a precipitator of their depression."[116]

Similarly, members of GenX tend to engage in the most self-destructive behaviors when under stress.[117] This generation has a high rate of alcohol abuse, and while it can be debated which cohort (BabyBoomers or GenXers) is more associated with illegal drug use, the fact is both cohorts participate in this particular destructive behavior. In *Baby Boomers Grow Up*, Whitbourne and Willis say of that generation "illicit drug and alcohol abuse…far exceed older cohorts."[118]

Contrary to popular belief, it has been shown that Millennials may have a better handle on dealing with stress than older generations (see Table 2).[119] They tend to employ non-traditional means of stress relief, as simple as listening to music, playing video games, or even surfing the Internet.[120] In addition, there is a better chance that a Millennial will turn to yoga or a meditation method to relieve stress.[121]

---

[114] Susan Krauss Whitbourne and Sherry L. Willis, *The Baby Boomers Grow Up: Contemporary Perspectives on Midlife* (Psychology Press, 2006), 120.

[115] Beth A. Kapes, "Depression and Baby Boomers: How Having it all May Be Too Much," accessed August 10, 2015, http://psychcentral.com/lib/depression-and-baby-boomers-how-having-it-all-may-be-too-much/.

[116] Ibid.

[117] "BeInkandescent: The Millennials and Health: How They Behave under Stress," accessed July 6, 2015, http://www.beinkandescent.com/articles/1014/stress+response.

[118] Whitbourne and Willis, *Baby Boomers Grow Up*.

[119] Ibid.

[120] Ibid.

[121] Ibid.

Table 2. Compulsive and Destructive Behavior Applicability

	Applies to Cohort?		
	BabyBoomers	GenX	Millennials
Compulsive and destructive behavior	Yes	Yes	--

Introversion

If the premise as stated in the article "How Digital Technology Is Creating a World of Introverts" is accepted, the digital world is creating a world that accommodates more introverts.[122] Such a world is one that, on Facebook, sees "398 million active users six out of seven days…300 million photos uploaded per day…and 3.2 billion 'likes' and comments' registering per day."[123] Additionally, on relationship sites such as eHarmony, Match, Christian Mingle, and others, it was found that "twice as many couples met through online dating sites than at social events, bars and clubs combined…one in six marriages and one in five committed relationships have been among those who connected via online dating."[124] Similarly, in the business networking website LinkedIn, there are "200 million individual members, over 2.8 million businesses, and 50 million unique visitors each week. And finally, instead of going to a traditional campus, students can take courses without ever meeting their fellow classmates or professors.[125]

[122] "How Digital Technology Is Creating a World of Introverts," SocialTimes, July 3, 2013, http://www.adweek.com/socialtimes/how-social-media-is-creating-a-world-of-introverts/131861.

[123] Ibid.

[124] Ibid.

[125] Ibid.

With the younger generation being more tech-savvy and "connected," it is reasonable to say they are more likely to be influenced by this technological isolation and, therefore, developmentally and socially more introverted than older, less technical generations.[126] This presents a paradox, in which today's introverted Millennials actually have far more contact with others than did introverts of previous generations. Susan Cain, a former corporate attorney, negotiations consultant, and author of *Quiet: The Power of Introverts in a World That Can't Stop Talking*, stated: "A wired world can be alienating…When we bathe in the blue light of our gadgets, we're doing many things: surfing, working, gaming and, yes, tuning out the world. But we're also hearing ideas from people whose voices might not have carried in the pre-wired era, who might not have broken through the chatter."[127] She continues, stating, "A distinct breed has emerged: call it the "offline introvert/online extrovert."[128] The characteristic of introversion then will apply to Millennials, but not to Baby Boomers or GenXers (see Table 3).

Table 3. Introversion Applicability

	Applies to Cohort?		
	BabyBoomers	GenX	Millennials
Introversion	--	--	Yes

[126] Ibid.

[127] Susan Cain, "Why Gadgets Are Great for Introverts," *TIME*, accessed August 12, 2015, http://ideas.time.com/2012/08/16/gadgets-are-great-for-introverts/.

[128] Ibid.

Rebellious, passive aggressive

As they near retirement age, the Baby Boomers are becoming less like the rebels of their youth (such as James Dean and Marlon Brando) and becoming more like the stereotypical "elder" generation, more prone to mentoring and passing on values than desiring to change the system.[129] Similarly, GenXers, being a largely "overlooked and forgotten generation," typically did not "rebel against anything or stand for much in their youth."[130] While this reflexively seems to be a somewhat obvious statement, it nonetheless underscores the analytical aspect of the cohort with respect to its rebelliousness.

Further, it demonstrates that the GenXers would be less inclined to act rebelliously. According to Strauss and Howe, Millennials will "rebel against the current culture in ways heretofore unimaginable to us today. They are destined to establish themselves as the anti-Boomers, remaking society into something as unrecognizable to aging Boomers as the 1960s were to their parents."[131] The fact is that Millennials are rebellious, but is that because the older generations have lost the rebelliousness of their youth and the Millennials have yet to reach that level of maturity? Or might it be because the in-your-face hippies of the 60s, the BabyBoomers, have successfully turned rebellion into the everyday norm, so their rebelliousness appears to be normal? Either way, with this characteristic analysis, the BabyBoomers and GenXers do not rise to the rebellious nature, but the Millennials do (see Table 4).

[129] William Strauss and Neil Howe*, Generations: The History of America's Future, 1584 to 2069* (New York: Quill, 1991), 60.

[130] "How Baby Boomers Screwed Their Kids—and Created Millennial Impatience," Salon, accessed July 6, 2015, http://www.salon.com/2014/01/04/how_baby_boomers_screwed_their_kids_%E2%80%94_and_created_Millennial_impatience/.

[131] William Strauss and Neil Howe*, Millennials Rising: The Next Great Generation* (New York: Random House, 2009).

Table 4. Rebellious, Passive Aggressive Applicability

	Applies to Cohort?		
	BabyBoomers	GenX	Millennials
Rebellious, Passive Aggressive	--	--	Yes

Ethical "flexibility"

According to the Ethics Resource Center (ERC) a "nonprofit organization devoted to the advancement of high ethical standards and practices in public and private institutions,"[132] younger workers have a higher probability of observing misconduct within a company, but reporting the misconduct is less likely to occur.[133] While Millennials share some ethics with the older generations, they are more likely to bend the ethics when it fits them. For example, they are more likely to keep copies of confidential documents, call in sick when they are not, or ignore a policy if they do not personally believe the policy to be right.[134] BabyBoomers and GenXers conversely are more inclined to toe the ethical line, making this characteristic one solely in the Millennial's column.[135] The data in Table 5 indicate this divide.

[132] "Ethics Resource Center," Wikipedia, last modified 11 June 2015. https://en.wikipedia.org/wiki/Ethics_Resource_Center

[133] Ethics Resource Center, *Millennials, Gen X and Baby Boomers: Who's Working at Your Company and What Do They Think About Ethics?* (Arlington, VA: Ethics Resource Center, 2010), http://ethics.org/files/u5/Gen-Diff.pdf.

[134] Ibid.

[135] Ibid.

Table 5. Ethical "Flexibility" Applicability

	Applies to Cohort?		
	BabyBoomers	GenX	Millennials
Ethical "flexibility"	--	--	Yes

Reduced loyalty

It can be said that loyalty is a two-way street. And while that may be true in theory and practice, the relevant loyalty in this characteristic is the employee to the organization. It is true that employers today cut back on employee benefits. Recent surveys indicate reductions in health coverage, pensions (today just twenty-four percent of employers surveyed provide a traditional pension plan open to all employees), retiree health insurance, long-term care insurance, education benefits, and even benefits for parents in the form of dependent care flexible spending accounts.[136] While these reductions may factor into why an employee's loyalty might wane, the analysis is concerned with which cohort has a reduced loyalty, not necessarily the root cause of that reduction.

When it comes to loyalty, BabyBoomers are strikingly the most loyal of the cohorts.[137] In other cohorts, however, the loyalty begins to fade. Interestingly, while GenX has been found to be more loyal to religion than other

[136] Forbes states that a business strategy for employers now is to have employees pay a higher percentage of the costs of what used to be benefits paid wholly by the employer; Emily Brandon, "Workplace Benefits That Are Disappearing," U.S. News, July 28, 2014, http://money.usnews.com/money/retirement/articles/2014/07/28/workplace-benefits-that-are-disappearing.

[137] "Younger Managers Rise in the Ranks: EY Study on Generational Shifts in the US Workplace," EY, accessed August 18, 2015, http://www.ey.com/US/en/Issues/Talent-management/Talent-Survey-The-generational-management-shift.; "Study: Work-Life Challenges across Generations, Millennials and Parents Hit Hardest," EY, accessed August 18, 2015, http://www.ey.com/US/en/About-us/Our-people-and-culture/EY-work-life-challenges-across-generations-global-study; Strauss and Howe, *Generations*.

generations,[138] they may "value their relationship with their co-workers above the relationship with their company, especially if this co-worker is a friend."[139] Additionally, giving the employer two-weeks' notice to a GenX employee could be their idea of being loyal to the company.

As for the Millennials, the same study finds that "the younger the generation, the least loyal the generation appeared to be. For instance … 65% of boomers, 40 percent of Xers, and 20 percent of Yers" (Millennials) reported that they would prefer to remain with their existing employer throughout their professional lives. Couple this with the ERC finding, which showed Millennials to be "less likely to be engaged and to see their long term future as being tied to their current employer."[140] However, once a boss has proven to a Millennial that he or she is a good boss, the Millennial typically becomes fiercely loyal to that boss, more so than the organization.[141]

While this point shows that Millennials can display loyalty, the insider threat betrays an organization, not a boss, so loyalty, for the purposes of this study, could be described as misplaced. Table 6 categorizes the generations' results.

[138] Christie Nicholson, "Generation X Loyaler to Religion than Previous Generation," Scientific American, August 28, 2010, http://www.scientificamerican.com/podcast/episode/generation-x-more-loyal-to-religion-10-08-28/.

[139] Anick Tolbize, "Generational Differences in the Workplace," Research and Training Center on Community Living, 2008, 6.

[140] "Millennials, Gen X and Baby Boomers," Ethics Resource Center.

[141] Vivian Giang, "How Millennials Really View Loyalty in the Workplace," Business Insider, September 17, 2012, http://www.businessinsider.com/how-millennials-really-view-loyalty-2012-9.

Table 6. Reduced Loyalty Applicability

	Applies to Cohort?		
	BabyBoomers	GenX	Millennials
Reduced loyalty	--	Yes	Yes

Entitlement and narcissism (ego/self-image)

This characteristic belongs to the BabyBoomers and Millennials. Recall from Chapter II that narcissism manifests itself with "arrogant behavior, a lack of empathy for other people, and a need for admiration—all of which must be consistently evident at work and in relationships."[142] In *Generations*, the authors describe the idealist generations, to which the BabyBoomer cohort has been attributed, as being "narcissistic rising adults" but makes no mention of its influence in later years. However, there is no indication that narcissistic traits ever stop influencing a person as they grow older. For that reason, the BabyBoomers will be counted as being narcissistic.[143]

Millennials, in turn, are described by EY (formerly Ernst and Young) as being "entitled and concerned primarily about individual promotion."[144] Jean M. Twenge, author of *Generation Me: Why Today's Young Americans Are More Confident, Assertive, Entitled—and More Miserable Than Ever before* says that Millennials have "more focus on the self and less focus on the group, society,

[142] "Narcissistic Personality Disorder," *Psychology Today*.

[143] Strauss and Howe, *Generations*, 87.

[144] Giang, Vivian, "Here are the Strengths and Weaknesses of Millennials, Gen X, and Boomers," Business Insider, September 9, 2013, http://www.businessinsider.com/how-Millennials-gen-x-and-boomers-shape-the-workplace-2013-9.

and community."[145] Additionally, in "Managing Millennials," Claire Raines states, "Gen-Xers complain the Millennials are another indulged generation like the Boomers—that they're self-absorbed and Pollyanna-ish"[146]

While there are no definitive studies indicating that GenXers as a group exhibit narcissism to the extent of the other cohorts, there are sufficient sources with statements such as "the narcissism epidemic has touched every American"[147] and "everyone exhibits some amount of narcissism,"[148] to include this generation as exhibiting narcissism as well (see Table 7).

Table 7. Entitlement/Narcissism (Ego/Self-image) Applicability

	Applies to Cohort?		
	BabyBoomers	GenX	Millennials
Entitlement/narcissism (ego/self-image)	Yes	Yes	Yes

Minimizing their mistakes or faults

When discussing the ability to recognize or admit their faults, the one cohort that weighs in below the others is the Millennials. Their overbearing "helicopter" parents spent their time convincing the Millennials that the youngsters are special, ensuring awards and trophies were presented for simply participating. Today, they minimize their mistakes and faults and, in doing so,

[145] Lauren Hansen and Ryu Spaeth, "Narcissistic, Broke, and 7 Other Ways to Describe the Millennial Generation [Updated]," The Week, April 18, 2013, http://theweek.com/articles/475383/narcissistic-broke-7-other-ways-describe-Millennial-generation-updated.

[146] Claire Raines, "Managing Millennials," 2002.

[147] Jean M Twenge and W. Keith Campbell, *The Narcissism Epidemic: Living in the Age of Entitlement* (New York: Simon and Schuster, 2009).

[148] Christopher Lasch, *The Culture of Narcissism: American Life in an Age of Diminishing Expectations* (New York: WW Norton & Company, 1991).

echo their upbringing. This has led them to believe that their mistakes actually were minimal, because the parents did not want to ruin their self-esteem.[149]

BabyBoomers also fall into this fault. They are drawing far more in terms of government programs than they contributed; they lived a life on fossil fuels and did not consider the damage it would wreak on the environment until recently.[150] Yet, for these shortfalls, one would be hard-pressed to read or hear any BabyBoomer in a position of power or authority readily admit that. Yes, they do decry the situation, but talk a collective "we" as a nation when disusing responsibility for those issues, rather than "we" as a collective generation.

The data in Table 8 illustrates these results.

Table 8. Minimizing Their Mistakes or Faults Applicability

	Applies to Cohort?		
	BabyBoomers	GenX	Millennials
Minimizing mistakes or faults	Yes	--	Yes

Inability to assume responsibility for their actions

When examining ability to "own up" to one's mistakes, the findings placed the Millennials in a positive light. Whether this is because they believe they are still learning their ropes or as a rule are more open, they are more willing to admit

[149] Susanne Goldstein, "3 Reasons Millennials Aren't Ready For Real Careers," Business Insider, August 17, 2012, http://www.businessinsider.com/3-reasons-millennials-arent-ready-for-real-careers-2012-8.

[150] In his 2011 book *The Pinch, how Baby Boomers Took Their Children's Future and Why They Should Give it Back*, David Willets shows that BabyBoomers receive benefits at the rate of 116% of what they contributed. A Cato Institute report states Baby Boomers "paid less of their earnings into Social Security than…Gen-X/Yers, yet they'll receive more in benefits" leaving GenX and Millennials to make up the difference.

to making a mistake than the older generations. Additionally, they expect their superiors to do the same.[151] While there is no definitive statement of GenXers or BabyBoomers being unwilling to assume responsibility for their actions, not finding sources stating they willingness, coupled with the Millennials' willingness, results in this characteristic being attributed to these cohorts (see Table 9).

Table 9. Inability to Assume Responsibility for Their Actions Applicability

	Applies to Cohort?		
	BabyBoomers	GenX	Millennials
Inability to assume responsibility for their actions	Yes	Yes	--

Intolerance of criticism

It can be argued that GenX, who coddled the Millennials, did so in an effort to compensate for their upbringing, where they were often left to fend for themselves, being the first generation of "latchkey" children and children in a single-parent household. Regardless of the reasoning, the results are not surprising. A *TIME* article used the term "teacup" generation when describing Millennials: outwardly, they present an air of perfection; inwardly, however, they are fragile and easily broken if not properly handled.[152] Because of this, not only are they intolerant toward criticism, but also, when presented with it, many

[151] Steve Cody, "Five Tips for Dealing with Millennials," Transworld Business, April 19, 2013, http://business.transworld.net/127471/news/five-tips-for-dealing-with-Millennials/.

[152] Jane Buckingham and Marcus Buckingham, "Note to Generation Y Workers: Performance on the Job Actually Matters," *TIME*, September 28, 2012, http://business.time.com/2012/09/28/note-to-gen-y-workers-performance-on-the-job-actually-matters/.

management consultants suggest sandwiching the criticism between positive affirmations. The analysis in Table 10 indicates these results.

Table 10. Intolerance of Criticism Applicability

	Applies to Cohort?		
	BabyBoomers	GenX	Millennials
Intolerance of criticism	--	--	Yes

Self-perceived value exceeds performance

When it comes to inflated self-worth, Millennials own the category. Millennials believe "trying hard plus meaning well deserve much credit and appreciation—that their results are far less important than the effort and good intention expended to produce them."[153] After all, this is what they were told growing up. Whether because of the previously mentioned helicopter parents telling them they can do no wrong, or "earning" a trophy for riding the bench on a last-place team, they have been told their whole lives that they are special, which has given them a skewed performance-to-value ratio. Far more Millennials (by a factor of 2) wanted to know when and how they could get a promotion when compared to GenXers and Boomers.[154]

[153] Bruce Sallan, "Constructive Criticism—Are Today's Millennials Too Thin-Skinned to Handle it?" Bruce Sallan: A Dad's Point-of-View, accessed July 6, 2015, http://www.brucesallan.com/2013/02/16/thin-skinned-can-todays-Millennials-handle-constructive-criticism/.

[154] "Younger Managers Rise in the Ranks: EY Study on Generational Shifts in the US Workplace," EY, accessed August 18, 2015, http://www.ey.com/US/en/Issues/Talent-management/Talent-Survey-The-generational-management-shift.; "Study: Work-Life Challenges across Generations, Millennials and Parents Hit Hardest," EY, accessed August 18, 2015, http://www.ey.com/US/en/About-us/Our-people-and-culture/EY-work-life-challenges-across-generations-global-study.

Lacking common perceptions, conventional wisdom, or, more importantly, any source material (academic or otherwise) indicating one way or another that BabyBoomers or GenXers possess this characteristic, "self-perceived value exceeds performance" is attributed to only the Millennials (see Table 11).

Table 11. Self-perceived Value Exceeds Performance Applicability

	Applies to Cohort?		
	BabyBoomers	GenX	Millennials
Self-perceived value exceeds performance	--	--	Yes

Lack of empathy

In a 2010 report on empathy that, over time, examined "changes…in a commonly used measure of dispositional empathy," it was reported that empathy is on the decline.[155] Within the medical profession, arguably one career path where empathy is necessary, "three longitudinal and six cross-sectional studies of medical students demonstrated a significant decrease in empathy."[156] Compared to the BabyBoomers, GenXers' and Millennials' "concern for others (e.g., empathy for outgroups…) declined."[157]

[155] Sara H. Konrath., Edward H. O'Brien, and Courtney Hsing. "Changes in dispositional empathy in American college students over time: A meta-analysis," *Personality and Social Psychology Review* 15, no. 2 (May 2011): 180–98. doi:10.1177/1088868310377395.

[156] Melanie Neumann, Melanie et al., "Empathy Decline and its Reasons: A Systematic Review of Studies with Medical Students and Residents," *Academic Medicine* 86, no. 8 (2011): 996–1009.

[157] Jean M. Twenge, Keith W. Keith Campbell, and Elise C. Freeman. "Generational Differences in Young Adults' Life Goals, Concern for Others, and Civic Orientation, 1966–2009," *Journal of Personality and Social Psychology* 102, no. 5 (2012): 1045.

Over the last 30 years, empathy has been on the decline; the younger the person, the less empathetic he or she tends to be.[158] Nothing exemplifies this more than the increasing occurrences of cyber bullying, found almost exclusively in the younger generations (Millennials and "Generation Z," which is not yet in the workplace, and so not part of the analysis). Only the BabyBoomers are seen to have empathy as a positive attribute (see Table 12).[159]

Table 12. Empathy Applicability

	Applies to Cohort?		
	BabyBoomers	GenX	Millennials
Lack of empathy	--	Yes	Yes

Predisposition toward law enforcement (authority)

When examining the generational attitudes toward authority, "both Xers and [Millennials] are comfortable with authority figures"; however, they are "are not impressed with titles or intimidated by them. They find it natural to interact with their superiors, unlike their older counterparts and to ask questions."[160] Millennial's tend to "value direction, leadership, and the authority that is based in know-how and experience…but resist the type of authority that originates in a

[158] Jamil Zaki, "What, Me Care? Young Are Less Empathetic," *Scientific American*, December 23, 2010, http://www.scientificamerican.com/article/what-me-care/.

[159] Christopher J. Einolf, "Will the Boomers Volunteer during Retirement? Comparing the Baby Boom, Silent, and Long Civic Dohorts," *Nonprofit and Voluntary Sector Quarterly* 38, no. 2 (2009): 181-199; Jean M. Twenge and Stacy M. Campbell, "Generational Differences in Psychological Traits and Their Impact on the Workplace," *Journal of Managerial Psychology* 23, no. 8 (2008): 862–877.

[160] Morley Winograd and Michael D. Hais, "The Millennials and Health: How They Behave Under Stress," BeInkandescent, June 2012. http://www.beinkandescent.com/articles/1014/stress+response.

'because I said so' attitude."[161] GenXers are said to have a "low level of trust toward authority" and large institutions.[162] BabyBoomers, on the other hand, have considerably better relationships "with parents, teachers, police, probation officers, and other authority figures."[163] With that in mind, this characteristic applies to the Millennials and GenXers (see Table 13).

Table 13. Predisposition toward Law enforcement (Authority) Applicability

	Applies to Cohort?		
	BabyBoomers	GenX	Millennials
Predisposition toward law enforcement (authority)	--	Yes	Yes

Tables 14 and 15 aggregate the individual tables that followed each factor summarizing the risk factors. These tables show, based on the analysis of available data, which cohort is most likely to possess insider threat potential and, by extension, to be a higher risk of becoming an insider threat. Table 14 calculates likelihood based solely on the total number of characteristics counted toward a given cohort. This table does not factor the relative importance of each factor.

[161] "Authority, Authoritarianism, and the Millennial Generation," LifeWay, February 19, 2015, http://www.lifeway.com/churchleaders/2015/02/19/authority-authoritarianism-and-the-Millennial-generation/.

[162] Cara Newman, "Boomers to Millennials: Generational Attitudes," Young Money, accessed July 6, 2015, http://finance.youngmoney.com/careers/boomers-to-Millennials-generational-attitudes/; "Who Is Generation X?," Jen X, accessed July 6, 2015, http://www.jenx67.com/who-is-generation-x.

[163] Marc. Freedman, *Prime time: How baby boomers will revolutionize retirement and transform America* (New York: Public Affairs, 2002.).

Table 14. Raw Tabulation

	Applies to Cohort?		
Characteristic	BB	GX	MIL
Greed/ financial need	Yes		Yes
Entitlement – narcissism (ego/self-image)	Yes	Yes	Yes
Ethical "flexibility"			Yes
Reduced loyalty		Yes	Yes
Rebellious, passive aggressive			Yes
Compulsive and destructive behavior	Yes	Yes	
Introversion			Yes
Lack of empathy		Yes	Yes
Predisposition towards law enforcement		Yes	Yes
Minimizing their mistakes or faults	Yes		Yes
Intolerance of criticism			Yes
Inability to assume responsibility for their actions	Yes	Yes	
Self-perceived value exceeds performance			Yes
Score (total count of "yes")	5	6	11

BB=BabyBoomers, GX=GenX, MIL=Millennials

Table 15 similarly calculates cohort cohort's likelihood to become an insider; beyond Table 14, however, Table 15 includes the established relative importance value to provide a more granular determination of the prediction.

Table 15. Weighted Tabulation

			BB		GX		MIL	
	Weight	Adjusted Score	Applies?	Adjusted Score	Applies?	Adjusted Score	Applies?	Adjusted Score
Greed/ financial need	1	1.0	yes	1.0			yes	1.0
Entitlement—narcissism (ego/self-image)	2	0.50	yes	0.5	Yes	0.5	yes	0.5
Ethical "flexibility"	3	0.33					yes	0.33
Vulnerability to blackmail	4	0.25	yes	0.25	yes	0.25	yes	0.25
Reduced loyalty	5	0.2			yes	0.2	yes	0.2
Rebellious, passive aggressive	6	0.17					yes	0.177
Compulsive and destructive behavior	7	0.14	yes	0.14	yes	0.14		
Introversion	8	0.13					yes	0.13
Lack of empathy	9	0.11			yes	0.11	yes	0.11

Table 15. Weighted Tabulation (cont'd)

			BB		GX		MIL	
	Weight	Adjusted Score	Applies?	Adjusted Score	Applies?	Adjusted Score	Applies?	Adjusted Score
Predisposition towards law enforcement	10	0.10			yes	0.10	yes	0.10
Minimizing their mistakes or faults	11	0.09	yes	0.09			yes	0.09
Intolerance of criticism	12	0.08					yes	0.08
Inability to assume responsibility for their actions	13	0.07	yes	0.07	yes	0.07		
Self-perceived value exceeds performance	14	0.07					yes	0.07
Total adjusted score			2.1899		1.0101		3.1609	

BB=BabyBoomers, GX=GenX, MIL=Millennials

As shown in Table 14, the "threat hierarchy" based on the cumulative score relative to the unweighted risk factors shows that the Millennials are the cohort with the highest risk of becoming an insider threat. Following that, the GenXers possess six risk factors to the BabyBoomers' five, indicating that they would be the next in the hierarchy, followed closely by the Boomers.

When applying the relative importance weights to the prediction, however, it provides a slightly different analytical view. While the Millennials still exhibit the highest insider threat potential, the BabyBoomers are clearly more likely than the GenXers to be a threat. This finding owes to the relative weights associated with the risk factors. As an example, the BabyBoomers, as outlined Chapter III, possess the factor of “greed/financial need,” while the GenXers do not. This is the highest-scored factor; so, while the GenXers have more total factors to their credit, the weights associated to them cause the hierarchy to be reversed for these two cohorts. While the relative ranks of the BabyBoomers compared to the GenXers is not the central theme in the thesis, it is interesting that applying relative weights to the factors can make such a significant differentiation in the calculations, emphasizing the need to have strong justifications for the relative weights.

This thesis asks, can it be stated that the generation of “Millennials” are collectively more likely to exhibit the characteristics and traits of an insider threat, and ultimately act in a similar manner, than previous generations? Based on the analysis of the risk factors and applying these to the cohorts, the answer to would appear to be yes; in fact, Millennials are more likely to become insider threats than other generations currently in the workforce.

THIS PAGE INTENTIONALLY LEFT BLANK

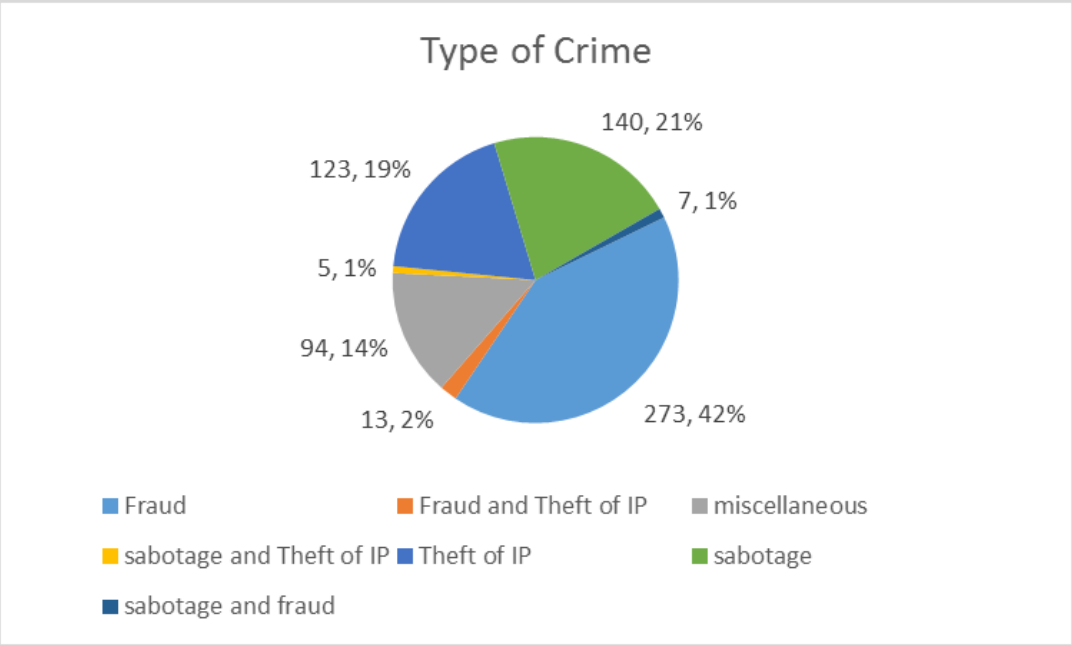
IV. INSIDER THREAT STATISTICS

Insider threat data has been collected from the Computer Emergency Response Team (CERT), a division of the Software Engineering Institute based at Carnegie Mellon University in Pittsburgh, Pennsylvania. While there is no regulatory requirement for any organization to report insider threat attacks to CERT, many organizations have done so. The data used for this analysis reaches back to 1997 and consists of 655 reported cases of an insider stealing data from within an organization's information systems. The data provides the type of attack (such as fraud or sabotage), the industry suffering the attack, and finally the year of the attack and the age of the attacker (allowing for generation cohort identification).

Figure 1 breaks down the type of crime, ranging from fraud to sabotage, committed by the various actors. Fraud, by far the largest category, is defined as "a form of theft/larceny that [occurs] when a person or entity takes money or property, or uses them in an illicit manner, with the intent to gain a benefit from it."[164] This category includes money laundering and identity theft, which are rapidly growing in popularity.

[164] "Fraud and Financial Crimes," FindLaw, accessed July7 2015, http://criminal.findlaw.com/criminal-charges/fraud-financial-crimes.html

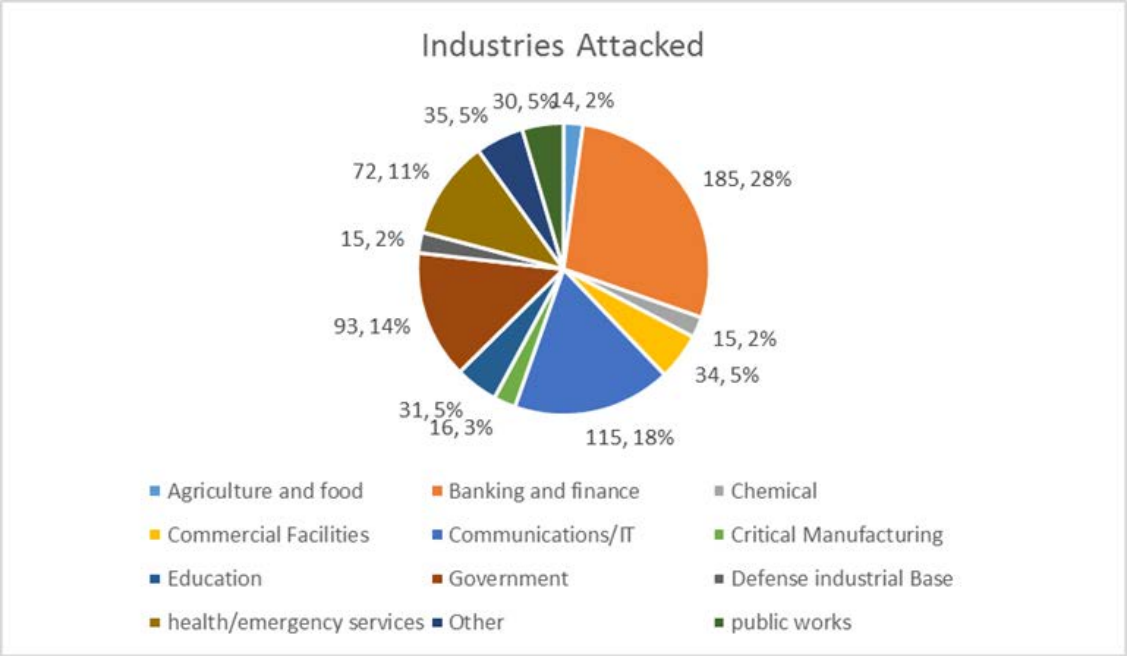
Figure 1. Types of Crime Committed by Insiders



The types of crimes committed by insiders, regardless of the industry. From Matt Collins (Insider Threat Researcher, CERT), email correspondence, May 12, 2015.

Figure 2 breaks the crimes down by the various industry sectors in which they occurred. Not surprisingly, as fraud is the most popular crime category, the banking and finance sector was the most common industry attacked.

Figure 2. Industries Attacked by Insiders



From Matt Collins (Insider Threat Researcher, CERT), email correspondence, May 12, 2015.

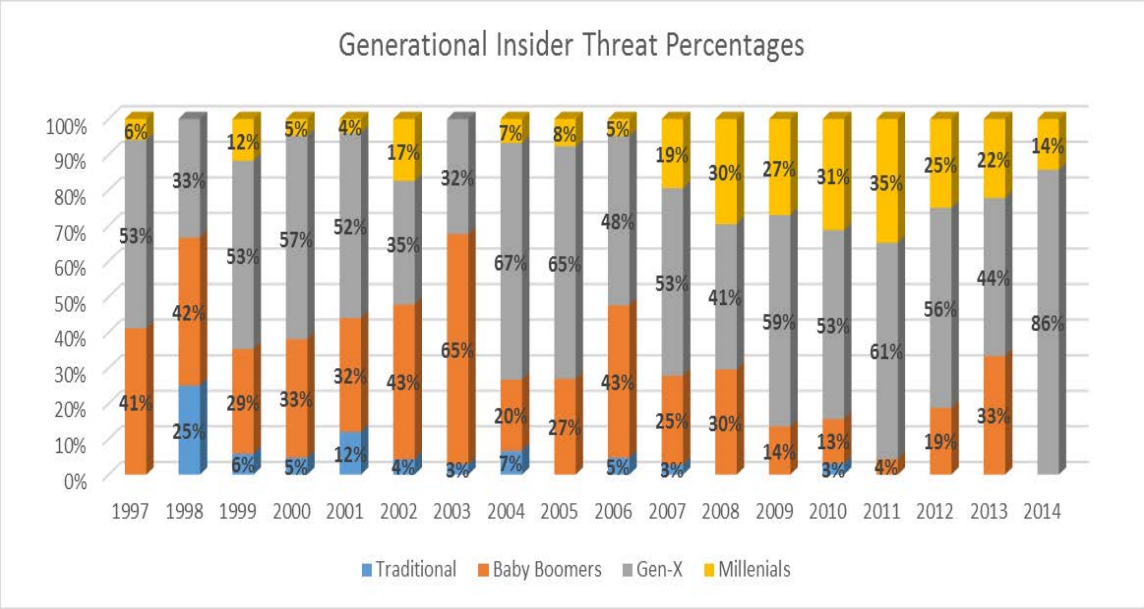
Figures 1 and 2 demonstrate that there are numerous industries affected by the insider threat, and the types of crime vary. This pattern, however, indicates a higher likelihood of fraud being committed within the financial sector. This study does not go into specific demographics regarding insiders' sex, age, or ethnicity, however a study from the Equal Employment Opportunity Commission (EEOC) states "there remains a large portion of establishments where these odds are unfavorable to women, African Americans, Hispanics and Asians."[165] Further analysis of the insider threat regarding insiders' sex, age, or ethnicity could provide valuable insight and allow specific industry sectors to be more vigilant regarding potential insiders.

Figure 3 shows the percentage of the successful insider attacks reported in a given year, broken down into the generations committing the acts. While the

[165] "Diversity In The Finance Industry", The U.S. Equal Employment Opportunity Commission, accessed 14 August, 2015, http://www1.eeoc.gov/eeoc/statistics/reports/finance/index.html

"traditional" generation is not part of this study, it has instances of compromises that have been eliminated from the insider threat concerns.

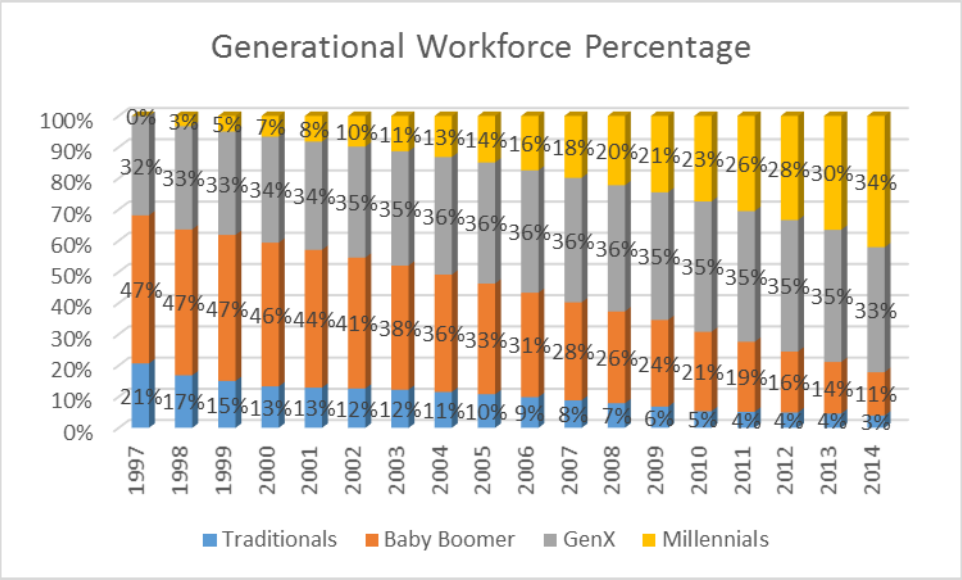
Figure 3. Generational Insider Threat Percentages



Percentage of insider attacks by generation from 1997 to 2014. From Matt Collins (Insider Threat Researcher, CERT), email correspondence, May 12, 2015.

Figure 4 shows the percentage of the workforce represented by each of this study's cohorts. Traditionals again are present in this representation, however in low and ever-decreasing numbers, indicating their minimal benefit to this study. The discernable pattern within this chart is the rapid growth of the Millennials in conjunction with the similarly rapid decline of the BabyBoomers, with the GenXers relatively unchanged throughout the 18 period being examined.

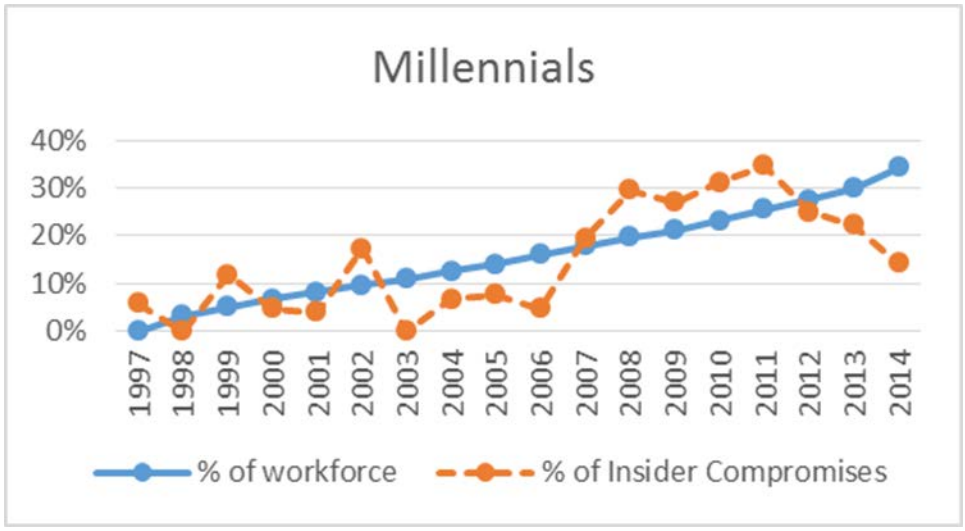
Figure 4. Generational Workforce Percentages



Percentage of the workforce represented by each generation. From Matt Collins (Insider Threat Researcher, CERT), email correspondence, May 12, 2015.

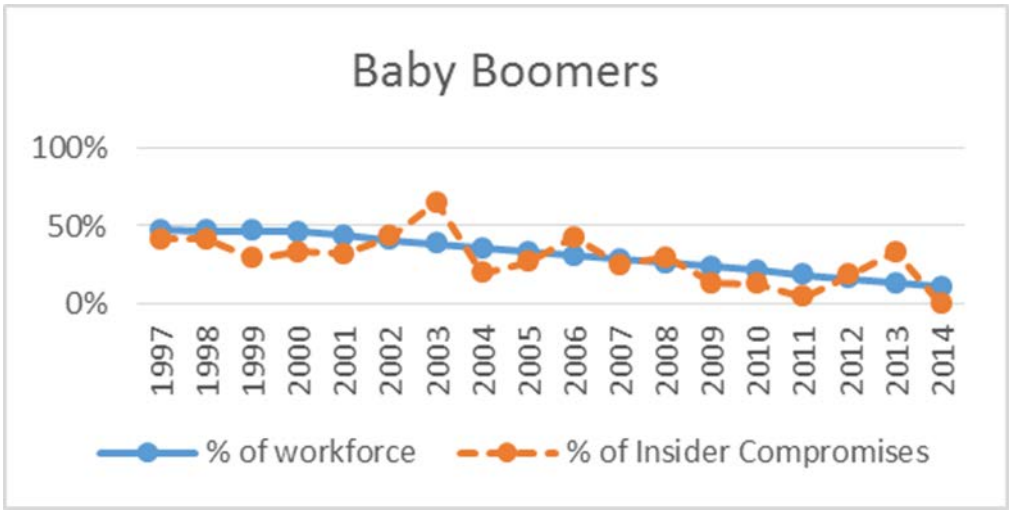
Figures 5–8 demonstrate the percentage of the workforce relative to a given cohort (solid blue line) along with the percentage of reported insider threat compromises (dashed orange line). The data shows that, as a rule, the Millennials' propensity to compromise data is, on average, commensurate with their representative percentage in the workforce (see Figure 5). BabyBoomers similarly perform as expected, given their workplace population (See Figure 6). The data in Figure 7 helps prove that the traditional generation can be eliminated from insider threat concerns. The Gen Xers' data, however, show that, regardless of their population in the workforce, they perform more than their proportionate share of compromises, contrary to the cohort hierarchy's suggestion (See Figure 8).

Figure 5. Millennial Breakdown



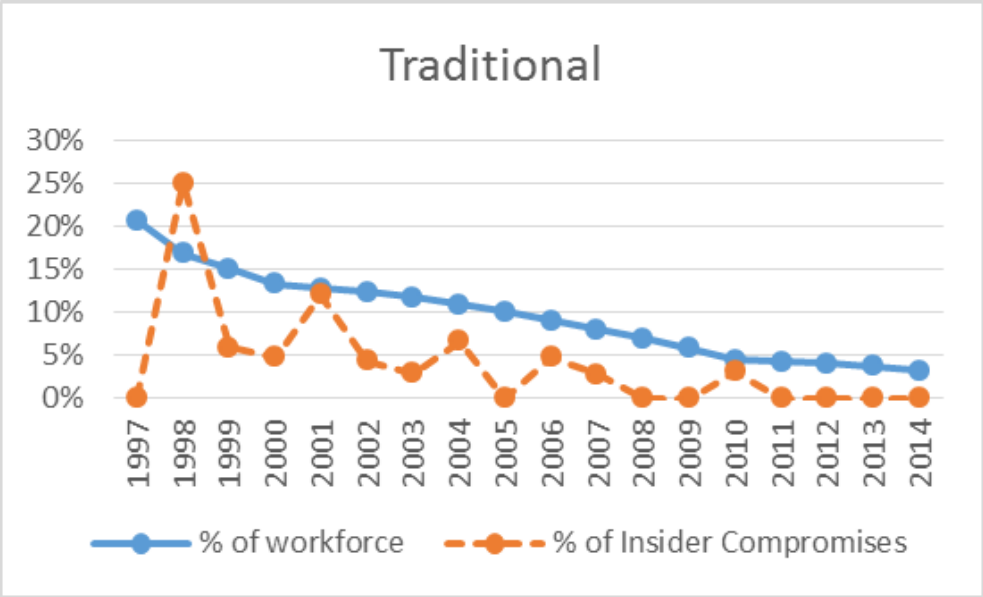
From Matt Collins (Insider Threat Researcher, CERT), email correspondence, May 12, 2015.

Figure 6. BabyBoomer Breakdown



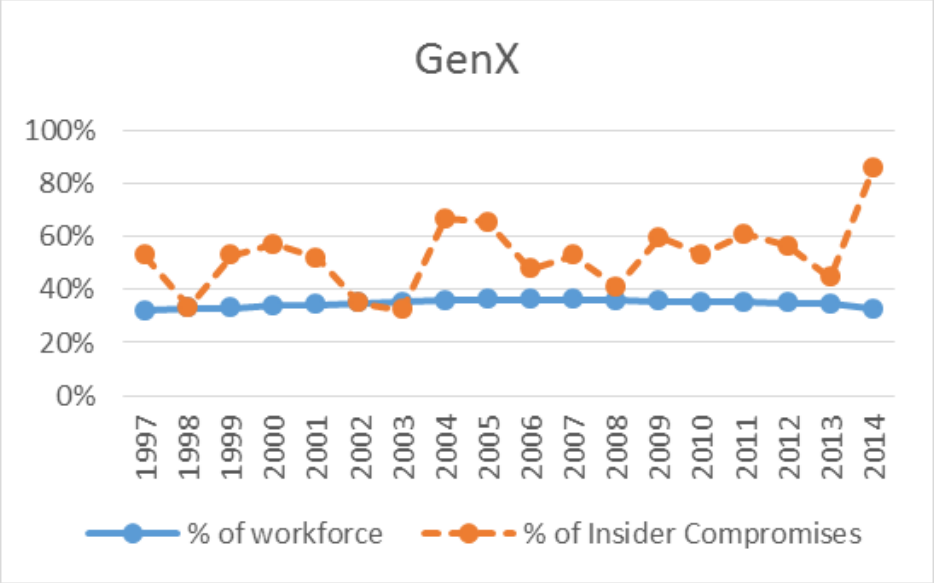
From Matt Collins (Insider Threat Researcher, CERT), in email correspondence, May 12, 2015.

Figure 7. Traditionals Breakdown



From Matt Collins (Insider Threat Researcher, CERT), in email correspondence, May 12, 2015.

Figure 8. GenX Breakdown



From Matt Collins (Insider Threat Researcher, CERT), in email correspondence, May 12, 2015.

The data in this figures conflict with the expected results based on the threat hierarchy established in the Chapter III. The disparate results are discussed in Chapter V.

V. CONCLUSION

This study comes to three general conclusions. The first conclusion is that, despite the stereotypes, Millennials are no more likely to be insider threats than any other generational cohort. Second, that, based simply on the projected representation in the workforce Millennials may still become the primary perpetrators of insider threat attacks in the workforce. Lastly, as their numbers in the workforce continue to grow, Millennials will likely be the majority of the perpetrators in the years to come; statistically, however, there is no reason to believe that the number of attacks will increase any more than what is currently experienced.

Table 16 shows that over the last five, ten, and eighteen years, the Millennials' average number of compromises relative to their workforce presence is 92 percent, 95 percent, and 93 percent, respectively.[166] Compared to the GenXers, who have compromised at a rate of 151 percent, 162 percent, and 176 percent relative to their workforce presence, it is evident that Millennials are not more of a security concern than older generations.

[166] Matt Collins (Insider Threat Researcher, CERT), email correspondence, May 12, 2015.

Table 16. Percentage of Compromises Compared to Workforce Population

		1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	Avg all	avg last 10 yrs	avg last 5 yrs
Millennials	% of workforce	0%	3%	5%	7%	8%	10%	11%	13%	14%	16%	18%	20%	21%	23%	26%	28%	30%	34%	16%	23%	28%
	% of Insider Compromises	6%	0%	12%	5%	4%	17%	0%	7%	8%	5%	19%	30%	27%	31%	35%	25%	22%	14%	15%	22%	26%
GenX	% of workforce	32%	33%	33%	34%	34%	35%	35%	36%	36%	36%	36%	36%	35%	35%	35%	35%	35%	33%	35%	35%	34%
	% of Insider Compromises	53%	33%	53%	57%	52%	35%	32%	67%	65%	48%	53%	41%	59%	53%	61%	56%	44%	86%	53%	57%	60%
Baby Boomer	% of workforce	47%	47%	47%	46%	44%	41%	38%	36%	33%	31%	28%	26%	24%	21%	19%	16%	14%	11%	32%	22%	16%
	% of Insider Compromises	41%	42%	29%	33%	32%	43%	65%	20%	27%	43%	25%	30%	14%	13%	4%	19%	33%	0%	28%	21%	14%

From Matt Collins (Insider Threat Researcher, CERT), email correspondence, May 12, 2015.

While it is true that, statistically, Millennials commit malicious insider crimes at a rate below their workforce presence (94 percent), they have surpassed GenXers as the largest percentage of the workforce, and are expected to become the majority of the workforce by 2016 (with estimates placing them as 75 percent of the workforce by 2025).[167] Assuming the Millennial workforce grows as predicted and that insider threat activities continue as they have in the last 18 years, this would mean that Millennials, by 2016, will account for 70 percent of insider threat compromises.

A. CRITICAL ASSESSMENT

During the course of researching, analyzing, and writing about this topic, it became apparent that there are several shortcomings that, while affecting the outcome to a minor extent, are not believed to cast any significant doubt on the outcome of the findings. Further research and analysis into this topic, specifically regarding these shortcomings, could address them sufficiently to buttress the findings and potentially strengthen the presented arguments.

The first shortcoming is the weight assigned to the fourteen insider threat risk factors. These risk factors were used to establish which generations are most likely to be insider threats. The weights were assigned based on input from available literature, both academic and Internet based. Information, however, was sparse, and so the weights are only estimates.

When comparing the data between the unweighted and weighted hierarchies, it became apparent that, in order to produce a valid and unbiased study, the weights should be derived by a group consensus rather than an individual one. Reassigning the relative weights would impact the hierarchy regarding the ranking of the BabyBoomers and GenXers. With that in mind, to further this study and add an element of peer consensus to it, a Delphi Method

[167] Schawbel, “Why You Can’t Ignore Millennials.”

with a panel of psychologists and cyber security experts providing would result in a more trustworthy ranking system.[168]

The second shortcoming is the actual data used in the analysis. The data was provided by CERT, a division of the Software Engineering Institute at Carnegie Mellon University. CERT is a "national asset in the field of cybersecurity that is recognized as a trusted, authoritative organization dedicated to improving the security and resilience of computer systems and networks."[169] It regularly assists "government, industry, law enforcement, and academia to develop advanced methods and technologies to counter large-scale, sophisticated cyber threats" and "works closely with the DHS to meet mutually set goals in areas such as data collection and mining, statistics and trend analysis, computer and network security, incident management, insider threat, software assurance, and more."[170] As recognized as CERT may be in the area of cyber security, CERT possesses no authority to require any organization, private or public, to report any breaches related to cyber security, yet alone specifics regarding compromises that can be traced directly to an insider threat. Some estimate that insider threats account for a large percentage of incidents.

A report by ClearSwift in 2013, for example, stated that "more than half of all security incidents (58 percent) can be attributed to the wider insider family: employees (33 percent), ex-employees (7 percent) and customers, partners or suppliers (18 percent)."[171] A study by the security group ISdecisions shows that 35 percent of the organizations with over 10,000 employees surveyed had

[168] Developed by RAND in the 1950s, the Delphi Method was created in the 1950s. The method consists of "a group of experts who anonymously reply to questionnaires and subsequently receive feedback in the form of a statistical representation of the 'group response,' after which the process repeats itself. The goal is to reduce the range of responses and arrive at something closer to expert consensus." See "Delphi Method", RAND, accessed August 31, 2015, http://www.rand.org/topics/delphi-method.html.

[169] "About Us," The CERT Division, accessed August 18, 2015, https://www.cert.org/about/.

[170] Ibid.

[171] "58% Information Security Incidents Attributed to Insider Threat," Infosecurity, May 3, 2013, http://www.infosecurity-magazine.com/news/58-information-security-incidents-attributed-to.

experienced an insider breach.[172] The 2013 report shows that, based on the replies to the survey questions, that there were an estimated 666,000 internal security compromises.[173] While knowing and being able to apply the details of a dataset of this magnitude would strengthen the validation of the analysis, this study could only use what was made available by CERT.

Lastly, the scope of this analysis is limited to only the generational cohorts. Furthering this study by breaking the cohorts into more specific demographics (e.g., age, race, gender, and level of education), while not providing significant validation to the findings, might provide further insight into the Millennial cohort itself to specifically determine which combination of demographics might need more observation. However, CERT reviewed cases between 1996 and 2006 and determined that there no statistically significant demographic commonalities based on the aforementioned demographic groups could be determined.[174]

B. CONCLUSION

This thesis has shown that Millennials are statistically less likely to become insider threats, and that closely examining the generation's demographics would aid this analysis.

So what does all of this mean to the cyber security community as they move forward and develop insider threat mitigation strategies? It means that, while Millennials have committed insider threat crimes below their representative workforce percentage, they will soon outnumber other generations. Their compromises, while proportionately lower, will outnumber other cohorts simply because of their sheer size, but not because they are any more prone to

[172] IS Decisions. "The Insider Threat Security Manifesto: Beating the Threat from within," IS Decisions, accessed July 22, 2015. http://www.isdecisions.com/resources/pdf/insiderthreatmanifesto.pdf.

[173] Ibid.

[174] Matt Collins (Insider Threat Researcher, CERT), email correspondence, May12, 2015.

compromise than the other cohorts. Successful mitigation steps should be developed, keeping this finding at the forefront of the strategy.

BIBLIOGRAPHY

About.com. “11 Tips for Managing Millennials.” Accessed January 1, 2015. http://humanresources.about.com/od/managementtips/a/millenials.htm.

Alcohol Rehab. “Generational Trends in Substance.” Accessed July 6, 2015. http://alcoholrehab.com/drug-addiction/substance-abuse-generational-trends/.

American Enterprise Institute. “The Events That Have Shaped the Millennial Era,” July 27, 2012. http://www.aei.org/publication/the-events-that-have-shaped-the-Millennial-era/.

American Medical Association. “About the Ethics Group.” Accessed August 14, 2015. http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/about-ethics-group.page?.

Asghar, Rob. “Gen X Is from Mars, Gen Y Is from Venus: A Primer on How to Motivate a Millennial.” January 14, 2014. Forbes. http://www.forbes.com/sites/robasghar/2014/01/14/gen-x-is-from-mars-gen-y-is-from-venus-a-primer-on-how-to-motivate-a-millennial/.

———. “What Millennials Want in the Workplace (and Why You Should Start Giving it to Them).” *Forbes*. January 13, 2014. http://www.forbes.com/sites/robasghar/2014/01/13/what-millennials-want-in-the-workplace-and-why-you-should-start-giving-it-to-them/.

Balkin, Alexander S. “Baby Boomers Ruined America: Why Blaming Millennials Is Misguided—and Annoying.” Salon. October 20, 2014. http://www.salon.com/2014/10/20}/baby_boomers_ruined_america_why_blaming_millennials_is_misguided_and_annoying/.

Boesler, Matthew. “Here’s What’s Really Going on with Baby Boomers and the Labor Force.” Business Insider. February 24, 2015. http://www.businessinsider.com/baby-boomers-are-retiring-2014-2.

Brandon, Emily. “Workplace Benefits That Are Disappearing.” *U.S. News & World Report*. July 28, 2014. http://money.usnews.com/money/retirement/articles/2014/07/28/workplace-benefits-that-are-disappearing.

Brickell, Claude. “Why Millennials Actually Support Edward Snowden (Whether They Know it or Not).” Thought Catalog. July 17, 2014. http://thoughtcatalog.com/claude-brickell/2014/07/why-Millennials-actually-support-edward-snowden/.

Buckingham, Jane and Marcus Buckingham. “Note to Generation Y Workers: Performance on the Job Actually Matters.” *TIME*.” September 28, 2012. http://business.time.com/2012/09/28/note-to-gen-y-workers-performance-on-the-job-actually-matters/.

Burton, Neel. “Is Greed Good?: The Psychology and Philosophy of Greed.” *Psychology Today*. October 6, 2014. https://www.psychologytoday.com/blog/hide-and-seek/201410/is-greed-good.

Cain, Susan. “Why Gadgets Are Great for Introverts,TIME.com.” Accessed August 12, 2015. http://ideas.time.com/2012/08/16/gadgets-are-great-for-introverts/.

Carter, Les. *Enough About You, Let’s Talk About Me: How to Recognize and Manage the Narcissists in Your Life*. 1st ed. Jossey-Bass, 2008.

The CERT Division. “About Us.” Accessed August 18, 2015. https://www.cert.org/about/.

The CERT Insider Threat Team. Unintentional Insider Threats: A Foundational Study (CMU-SEI-2013-TN-022). Pittsburgh, PA: Carnegie Mellon University, 2013. http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf.

Clayton, Mark. “Bradley Manning Case Signals U.S. Vulnerability to ‘Insider’ Cyberattack.” The Christian Science Monitor. December 22, 2011. http://www.csmonitor.com/USA/2011/1222/Bradley-Manning-case-signals-US-vulnerability-to-insider-cyberattack.

Kendra Cherry. “What Are the Five Major Personality Traits?” About Education, Accessed July 16, 2015. http://psychology.about.com/od/personalitydevelopment/a/bigfive.htm.

Cisco. Data Leakage Worldwide *White Paper: The High Cost of Insider Threats* (C11-506224-00). San Jose, CA: Cisco Systems, 2008. http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.pdf.

Coaching Positive Performance. “8 Examples of Passive Aggressive Behaviour.” Accessed August 18, 2015. http://www.coachingpositiveperformance.com/8-examples-passive-aggressive-behaviour/.

Cody, Steve. “Five Tips for Dealing with Millennials,” Transworld Business. Accessed July 6, 2015. http://business.transworld.net/127471/news/five-tips-for-dealing-with-millennials/.

Cohn, D’vera and Paul Taylor. “Baby Boomers Approach 65 – Glumly.” Pew Research Center. December 20, 2010. http://www.pewsocialtrends.org/2010/12/20/baby-boomers-approach-65-glumly/.

Colby, Sandra L., and Jennifer M. Ortman. *The Baby Boom Cohort in the United States: 2012 to 2060* (P25-1141). Washington, DC: United States Census Bureau, 2014. http://www.census.gov/content/dam/Census/library/publications/2014/demo/p25-1141.pdf.

Cole, Eric. *Insider Threats in Law Enforcement*. Bethesda, MD: SANS Institute, 2014. http://www.sans.org/reading-room/whitepapers/analyst/insider-threats-law-enforcement-35402.

Cornerstone Business Solutions. “Gen-X Is Getting Older.” Accessed February 7, 2015. http://www.cornerstoneresults.com/RefLib/KnlgeBk/mrkt_mr_gen-x_is_getting_older.htm.

Cramer, Reid. “Millennials Rising: Coming of Age in the Wake of the Great Recession.” New America. 2014. http://www.newamerica.org/downloads/Millennials_Rising_Coming_of_Age_in_the_Wake_of_the_Great_Recession.pdf.

Defense Human Resource Activity. “Opportunities and Motivation Are Increasing.” Accessed June 15, 2015. http://www.dhra.mil/perserec/osg/counterintelligence/opportunity-motive.htm#Increasing%20Opportunity.

“Defining Characteristics of Generational Cohorts - Participant Packet Intergen Dynamics.pdf.” PowerPoint. Accessed June 16, 2015.

Democracy Now! “‘Edward Snowden Is a Patriot’: Ex-NSA CIA, FBI and Justice Whistleblowers Meet Leaker in Moscow.” October 14, 2013. http://www.democracynow.org/2013/10/14/edward_snowden_is_a_patriot_ex.

Dictionary.com. “Loyal.” Accessed May 27, 2015. http://dictionary.reference.com/browse/loyal.

Dimock, Michael, Jocelyn Kiley, Scott Keeter, Carroll Doherty, and Alec Tyson. *Beyond Red vs. Blue: The Political Typology*. Washington, DC: Pew Research Center, 2014. http://www.people-press.org/files/2014/06/6-26-14-Political-Typology-release1.pdf.

Einolf, Christopher J. “Will the Boomers Volunteer during Retirement? Comparing the Baby Boom, Silent, and Long Civic Cohorts.” *Nonprofit and Voluntary Sector Quarterly* 38, no. 2 (2009): 181–199. http://nvs.sagepub.com/content/38/2/181.short.

Ethics Resource Center. *Millennials, Gen X and Baby Boomers: Who’s Working at Your Company and What Do They Think About Ethics?* Arlington, VA, Ethics Resource Center, 2010. http://ethics.org/files/u5/Gen-Diff.pdf.

EY. “Study: Work-Life Challenges across Generations, Millennials and Parents Hit Hardest.” Accessed August 18, 2015. http://www.ey.com/US/en/About-us/Our-people-and-culture/EY-work-life-challenges-across-generations-global-study.

———. “Younger Managers Rise in the Ranks: EY Study on Generational Shifts in the U.S. Workplace.” Accessed August 18, 2015. http://www.ey.com/US/en/Issues/Talent-management/Talent-Survey-The-generational-management-shift.

Fast Company. “Millennials Will Become the Majority in the Workforce In 2015. Is Your Company Ready?,” accessed February 4, 2015, http://www.fastcoexist.com/3037823/Millennials-will-become-the-majority-in-the-workforce-in-2015-is-your-company-ready.

FBI. “The Insider Threat.” Accessed June 15, 2015. https://www.fbi.gov/about-us/investigate/counterintelligence/insider_threat_brochure.

———. “Robert Philip Hanssen Espionage Case.” April 19, 2003. https://www.fbi.gov/about-us/history/famous-cases/robert-hanssen.

FindLaw. “Fraud and Financial Crimes.” Accessed July7 2015. http://criminal.findlaw.com/criminal-charges/fraud-financial-crimes.html

Fisher, Andrea. “How Digital Technology Is Creating a World of Introverts.” SocialTimes.” July 3, 2013. http://www.adweek.com/socialtimes/how-social-media-is-creating-a-world-of-introverts/131861.

Fox News. “Army: Fort Hood Gunman in Custody after 12 Killed, 31 Injured in Rampage.” November 6, 2009. http://www.foxnews.com/story/2009/11/06/army-fort-hood-gunman-in-custody-after-12-killed-31-injured-in-rampage.html.

———. “Target Says 40 Million Credit, Debit Card Accounts May Be Affected by Data Breach.” December 19, 2013. http://www.foxnews.com/us/2013/12/19/target-says-40m-accounts-may-be-affected-by-data-breach/.

Franconeri, Sabrina and Joe Maguire. “Associate Evaluations...the Next Generation.” *Law Practice Today* (April 2013). http://www.americanbar.org/content/dam/aba/publications/law_practice_today/associate-evaluations-the-next-generation.authcheckdam.pdf.

Freebase. “Compulsive Behavior.” Accessed August 18, 2015. https://www.freebase.com/m/0281lfw.

Freedman, Marc. *Prime Time: How Baby Boomers Will Revolutionize Retirement And Transform America*. New York: PublicAffairs, 2008.

Fry, Richard. “Millennials Surpass Gen Xers as the Largest Generation in U.S. Labor Force.” Pew Research Center. May 11, 2015. http://www.pewresearch.org/fact-tank/2015/05/11/millennials-surpass-gen-xers-as-the-largest-generation-in-u-s-labor-force/.

———. “This Year, Millennials Will Overtake Baby Boomers.” Pew Research Center. January 16, 2015. http://www.pewresearch.org/fact-tank/2015/01/16/this-year-millennials-will-overtake-baby-boomers/.

Gellman, Barton. “Edward Snowden, after Months of NSA Revelations, Says His Mission’s Accomplished - The Washington Post.” Accessed August 10, 2015. https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html.

“Generational Differences Chart.” West Midland Family Center. Accessed June 16, 2015. http://www.wmfc.org/uploads/GenerationalDifferencesChart.pdf.

Giang, Vivian. “Here are the Strengths and Weaknesses of Millennials, Gen X, and Boomers.” Business Insider. September 9, 2013. http://www.businessinsider.com/how-millennials-gen-x-and-boomers-shape-the-workplace-2013-9.

———. “How Millennials Really View Loyalty in the Workpalce.” Business Insider.” September 17, 2012. http://www.businessinsider.com/how-millennials-really-view-loyalty-2012-9.

Goldstein, Susanne. “3 Reasons Millennials Aren’t Ready For Real Careers.” Business Insider. August 17, 2012. http://www.businessinsider.com/3-reasons-millennials-arent-ready-for-real-careers-2012-8.

Goodin, Dan. “Epic Target Hack Reportedly Began with Malware-Based Phishing Email.” *Ars Technica*. February 12, 2013. http://arstechnica.com/security/2014/02/epic-target-hack-reportedly-began-with-malware-based-phishing-email/.

Good Therapy. “Sensitivity to Criticism.” Accessed May 27, 2015. http://www.goodtherapy.org/therapy-for-sensitivity.html.

Green, Chloe. “Knowledge Is Power, Data Is Money.” Information Age. December 4, 2014. http://www.information-age.com/industry/uk-industry/123458725/knowledge-power-data-money.

Hansen, Lauren and Ryu Spaeth. “Narcissistic, Broke, and 7 Other Ways to Describe the Millennial Generation [Updated].” The Week. April 18, 2013. http://theweek.com/articles/475383/narcissistic-broke-7-other-ways-describe-millennial-generation-updated.

Hattem, Julian. “Target Hack Cost Banks over $200M.” The Hill. Accessed February 18, 2014. http://thehill.com/policy/technology/198634-target-hack-cost-banks-over-200m.

Harding, Luke. “How Edward Snowden Went from Loyal NSA Contractor to Whistleblower.” *The Guardian*, February 1, 2014. http://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract.

Heuer, Richards J. “Insider Espionage Threat.” U.S. Department of Agriculture. Accessed August 18, 2015. http://www.dm.usda.gov/ohsec/pdsd/Security%20Guide/Treason/Insider.htm.

Horbury, Andrew. “The Rise of Hacktivism and Insider Threats.” Symantec. February 17, 2014. http://www.slideshare.net/NortonSecuredUK/symantec-the-rise-of-hacktivism-and-insider-threats.

Huffington Post. “Millennial Generation Money-Obsessed And Less Concerned With Giving Back, Study Finds.” March 16, 2012. http://www.huffingtonpost.com/2012/03/16/millennial-generation-study-fame-money_n_1354028.html.

Hurd, Michael J. “The Psychology of Loyalty (DE Wave), Living Resources Center.” Accessed May 27, 2015. https://drhurd.com/the-psychology-of-loyalty-de-wave/.

Infosecurity. “58% Information Security Incidents Attributed to Insider Threat.” May 3, 2013. http://www.infosecurity-magazine.com/news/58-information-security-incidents-attributed-to.

IS Decisions. “The Insider Threat Security Manifesto: Beating the Threat from within.” Accessed July 22, 2015. http://www.isdecisions.com/resources/pdf/insiderthreatmanifesto.pdf.

Internet Encyclopedia of Philosophy. “Ethics.” Accessed August 14, 2015. http://www.iep.utm.edu/ethics /.

Investopedia. “Business Ethics Definition.” Accessed August 14, 2015. http://www.investopedia.com/terms/b/business-ethics.asp.

Jen X. “Who Is Generation X?.” Accessed July 6, 2015. http://www.jenx67.com/who-is-generation-x.

Johnson, Jeffrey G., Patricia Cohen, Joceyln Brown, Elizabeth M. Smailes, and David P. Bernstein (July 1999), “Childhood Maltreatment Increases Risk for Personality Disorders during Early Adulthood.” *Archives of Psychiatry* 56, no. 7(July 1999): 600–6.

Kapes, Beth A. “Depression and Baby Boomers: How Having It All May Be Too Much.” Psych Central. Accessed August 10, 2015, http://psychcentral.com/lib/depression-and-baby-boomers-how-having-it-all-may-be-too-much/

Keene, Douglas L., Rita R. Handrich. “Generation X Members Are ‘Active, Balanced and Happy.’ Seriously?” November 29, 2011. http://www.thejuryexpert.com/2011/11/gen-x-members-are-active-balanced-and-happy/.

Keeney, Michelle, Eileen Kowalski, Dawn Cappelli, Andrew Moore, Timothy Shimeall, and Stephanie Rogers. *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*. United States Secret Service and Carnegie Mellon University, May 2005. http://www.secretservice.gov/ntac/its_report_050516.pdf.

Kirkpatrick, Shelley A. “Refining Insider Threat Profiles.” *Security* 45, no. 9 (September 2008): 56, 58, 60, 62–63.

Kreger, Randi. “Lack of Empathy: The Most Telling Narcissistic Trait.” *Psychology Today*. January 24, 2012. https://www.psychologytoday.com/blog/stop-walking-eggshells/201201/lack-empathy-the-most-telling-narcissistic-trait.

Konrath, Sara H., Edward H. O’Brien, and Courtney Hsing. “Changes in Dispositional Empathy in American College Students over Time: A Meta-Analysis.” *Personality and Social Psychology Review* 15, no. 2 (May 2011): 180–98. doi:10.1177/1088868310377395.

Kotlikoff, Laurence J. “Baby Boomers: The Greediest Generation.” *Forbes*. November 11, 2010. http://www.forbes.com/2010/11/11/greedy-boomers-social-security-medicare-cuts-personal-finance-kotlikoff.html.

Ladenson, Robert F. “Scientific and Technical Information, National Security, and the First Amendment: A Jurisprudential Inquiry.” *Public Affairs Quarterly* 1, no. 2 (April 1987): 1–20. http://www.jstor.org/stable/40435639.

Lasch, Christopher. *The Culture of Narcissism: American Life in an Age of Diminishing Expectations.* New York: WW Norton & Company, 1991.

Lifecourse. “Generational Archetypes.” Accessed June 16, 2015. http://www.lifecourse.com/about/method/generational-archetypes.html.

LifeWay. “Authority, Authoritarianism, and the Millennial Generation.” February 19, 2015. http://www.lifeway.com/churchleaders/2015/02/19/authority-authoritarianism-and-the-millennial-generation/.

Live Science. “Understanding the 10 Most Destructive Human Behaviors.” May 13, 2011. http://www.livescience.com/14152-destructive-human-behaviors-bad-habits.html.

Madar, Chase. “WikiLeaks, Manning and the Pentagon: Blood on Whose Hands?,” June 20, 2014. http://www.aljazeera.com/indepth/opinion/2012/01/2012121123135872284.html.

McClam, Erin. “‘Naive and Gravely Mistaken’: Analysts Rebut Snowden Claims.” NBC News. May 28, 2014. http://www.nbcnews.com/feature/edward-snowden-interview/naive-gravely-mistaken-analysts-rebut-snowden-claims-n117101.

Meek, James Gordon, Luis Martinez, and Alexander Mallin. “Intel Heads: Edward Snowden Did ‘Profound Damage’ to U.S. Security.” ABC News. January 29, 2014. http://abcnews.go.com/Blotter/intel-heads-edward-snowden-profound-damage-us-security/story?id=22285388.

MetLife Mature Market Institute. “Demographic Profile: America’s Gen X.” Accessed February 7, 2015. https://www.metlife.com/assets/cao/mmi/publications/Profiles/mmi-gen-x-demographic-profile.pdf.

Miller, Kathleen and Gopal Ratnam. “Shooter with Clearance Post-Arrest Exposes Vetting Gaps.” Bloomberg Business. September 18, 2013. http://www.bloomberg.com/news/articles/2013-09-18/shooter-with-clearance-post-arrest-exposes-vetting-gaps.

Moore, Carl. “Fun, Fun, Fun— Millennials Want to Have Fun at Work.” February 28, 2013. *Forbes*. http://www.forbes.com/sites/karlmoore/2013/02/28/fun-fun-fun-young-people-want-to-have-fun-at-work/.

National Cybersecurity and Communications Integration Center. *Combating the Insider Threat*. Washington, DC: U.S. Department of Homeland Security, 2014. https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat.pdf.

“National Insider Threat Task Force Mission Fact Sheet,” n.d. http://www.ncsc.gov/nittf/docs/National_Insider_Threat_Task_Force_Fact_Sheet.pdf.

Neumann M, F Edelhäuser, D Tauschel, MR Fischer, M Wirtz, C Woopen, A Haramati, and C Scheffer. “Empathy Decline and Its Reasons: A Systematic Review of Studies with Medical Students and Residents.,” August 2011. http://www.ncbi.nlm.nih.gov/pubmed/21670661.

Newman, Cara. “Boomers to Millennials: Generational Attitudes.” Young Money. Accessed July 6, 2015. http://finance.youngmoney.com/careers/boomers-to-millennials-generational-attitudes/.

Nicholson, Christie. “Generation X Loyaler to Religion than Previous Generation.” Scientific American.” August 28, 2010. http://www.scientificamerican.com/podcast/episode/generation-x-more-loyal-to-religion-10-08-28/.

Olguin, Michael, “5 Tips for Managing Millennial Employees.” Inc.” April 13, 2012. http://www.inc.com/michael-olguin/5-tips-for-managing-millennial-employees.html.

Poulsen, Kevin and Kim Zet. “WikiLeaks’ 400,000 Iraq War Documents Reveal Torture, Civilian Deaths,” Wired, October 22, 2010. http://www.wired.com/2010/10/wikileaks-press/.

Pearce, Gervase, and Peter Saul. “CMVH Military Health Ethics Think Tank Report: Towards a Framework for Military Health Ethics. IMIA Centre for Strategic Business Studies. Accessed August 14, 2015. http://www.camvh.org.au/ThinkTank/CMVH2006ThinkTankReport.pdf.

Primeast. “How to Lead the Millennial,” Accessed February 7, 2015. http://www.primeast.com/news/how-lead-millennial.

Psych Central. “Narcissistic Personality Disorder Symptoms.” Accessed August 18, 2015. http://psychcentral.com/disorders/narcissistic-personality-disorder-symptoms.

Psychology Dictionary. “What Is Minimization?.” Accessed May 25, 2015. http://psychologydictionary.org/minimization/.

Psychology Glossary. “Introvert (Introversion).” Accessed September 2, 2015. http://www.alleydog.com/glossary/definition.php?term=Introvert%20(Introversion).

Psychology Today. “Compulsive Behaviors.” Accessed August 18, 2015. https://www.psychologytoday.com/basics/compulsive-behaviors.

———. “Narcissistic Personality Disorder.” Last modified February 17, 2015. https://www.psychologytoday.com/conditions/narcissistic-personality-disorder.

Raines, Claire. “Generations at Work: Human Resource Management, Generation and Diversity, Generation Definition.” Accessed February 9, 2015.

Raines, Claire. “Managing Millennials.” 2002.

Rikleen, Lauren Stiller. “How the ‘Millennial’ Generation Works.” American Bar Association. Accessed February 15, 2015. http://www.americanbar.org/publications/young_lawyer_home/young_lawyer_archive/yld_tyl_may08_rikleen.html.

Salam, Reihan. “The Snowdenites Are Winning.” February 26, 2015. http://www.slate.com/articles/news_and_politics/politics/2015/02/edward_snowden_citizenfour_the_former_contractor_sparked_a_movement_that.html.

Sallan, Bruce. “Constructive Criticism—Are Today’s Millennials Too Thin-Skinned to Handle it?” Bruce Sallan: A Dad’s Point-of-View. Accessed July 6, 2015. http://www.brucesallan.com/2013/02/16/thin-skinned-can-todays-millennials-handle-constructive-criticism/.

Schawbel, Dan. “Why You Can’t Ignore Millennials.” *Forbes*. September 4, 2013. http://www.forbes.com/sites/danschawbel/2013/09/04/why-you-cant-ignore-millennials/.

Seltzer, Leon F. “Greed: The Ultimate Addiction.” *Psychology Today*. October 17, 2012. https://www.psychologytoday.com/blog/evolution-the-self/201210/greed-the-ultimate-addiction.

———. “The Narcissist’s Dilemma: They Can Dish it out But …” *Psychology Today*. October 12, 2011. https://www.psychologytoday.com/blog/evolution-the-self/201110/the-narcissists-dilemma-they-can-dish-it-out.

Shlackman, Jed. “Psychology, Spirituality, and the Manipulation of Human Society.” Examiner. June 9, 2013. http://www.examiner.com/article/psychology-spirituality-and-the-manipulation-of-human-society.

Sinek, Simon. “How Baby Boomers Screwed their Kids—and Created Millennial Impatience.” Salon. January 4, 2014. http://www.salon.com/2014/01/04/how_baby_boomers_screwed_their_kids_%E2%80%94_and_created_millennial_impatience/.

Simon, George. “Minimization: Trivializing Behavior as a Manipulation Tactic.” Counseling Resource. Accessed May 27, 2015. http://counsellingresource.com/features/2009/02/23/minimization-manipulation-tactic/.

Smith, Bianca. “What’s in it for Me?: The Fickle Heartbeat.” April 26, 2015. http://thefickleheartbeat.com/2015/04/26/whats-in-it-for-me/.

Strauss, William and Neil Howe. *Generations: The History of America’s Future, 1584 to 2069*. New York: Quill, 1991.

———*. Millennials Rising: The Next Great Generation*. New York: Random House, 2009.

Tanner, Robert. “15 Influential Events That Shaped Generation Y.” Management Is a Journey. Accessed February 15, 2015. http://managementisajourney.com/15-influential-events-that-shaped-generation-y-infographic/.

Thompson, D. “Political Ethics.” In *International Encyclopedia of Ethics*, edited by Hugh LaFollette. Oxford: Wiley-Blackwell, 2013. http://scholar.harvard.edu/files/dft/files/political_ethics-revised_10-11.pdf.

Taylor, Paul and George Gao. “Generation X: America’s Neglected ‘Middle Child.’” Pew Research Center. June 5, 2014. http://www.pewresearch.org/fact-tank/2014/06/05/generation-x-americas-neglected-middle-child/.

Thiefoldt, Diane and Devon Scheef. “Generation X and the Millennials: What You Need to Know about Mentoring the New Generations.” Law Practice Today. August 2004. http://apps.americanbar.org/lpm/lpt/articles/mgt08044.html.

Tolbize, Anick. “Generational Differences in the Workplace.” *Research and Training Center on Community Living*, 2008, 1–21.

Toobin, Jeffry. “Edward Snowden Is No Hero.” *New Yorker*. June 10, 2013. http://www.newyorker.com/news/daily-comment/edward-snowden-is-no-hero.

Twenge, Jean M. and Keith W Campbell. *The Narcissism Epidemic: Living in the Age of Entitlement.* New York: Simon and Schuster, 2009.

Twenge, Jean M. and Stacy M Campbell. "Generational Differences in Psychological Traits and Their Impact on the Workplace." *Journal of Managerial Psychology* 23, no. 8 (2008): 862–77.

U.S. News & World Report. "5 Workplace Stereotypes about Millennials That Aren't True." March 16, 2015. http://money.usnews.com/money/blogs/outside-voices-careers/2015/03/16/5-workplace-stereotypes-about-millennials-that-arent-true.

Value Options. "Baby Boomer Characteristics." Accessed June 16, 2015. http://www.valueoptions.com/spotlight_YIW/baby_boomers.htm.

Walden University. "Social Change Impact Report." 2011. http://www.waldenu.edu/~/media/Files/WAL/about/walden-university-social-change-impact-report-summary-report.pdf.

"What You Think about Millennials Is Wrong - The Washington Post." Accessed July 7, 2015. http://www.washingtonpost.com/blogs/on-leadership/wp/2015/02/23/what-you-think-about-millennials-is-wrong/.

Whitbourne, Susan Krauss and Sherry L. Willis. *The Baby Boomers Grow Up: Contemporary Perspectives on Midlife.* Psychology Press, 2006.

Whitson, Signe. "10 Things Passive Aggressive People Say," *Psychology Today*. Accessed August 18, 2015. https://www.psychologytoday.com/blog/passive-aggressive-diaries/201011/10-things-passive-aggressive-people-say.

Winograd, Morley and Michael D. Hais. "The Millennials and Health: How They Behave Under Stress." BeInkandescent. June 2012. http://www.beinkandescent.com/articles/1014/stress+response.

Zaki, Jamil. "What, Me Care? Young Are Less Empathetic." *Scientific American*. December 23, 2010. http://www.scientificamerican.com/article/what-me-care/.

Zeiger, Elise R. "Millennials Need Fun, Flexibility at Work." CNN.com. July 20, 2011. http://www.cnn.com/2011/LIVING/07/20/hot.schedules.millenials/.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California